МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЛІНГВІСТИЧНИЙ УНІВЕРСИТЕТ
Кафедра менеджменту і маркетингу

Кваліфікаційна робота магістра

на тему: «ІНФОРМАЦІЙНА БЕЗПЕКА БІЗНЕСУ СУЧАСНОЇ ОРГАНІЗАЦІЇ»
(на прикладі ТОВ «ІНКОМ-ІНВЕСТ»)

Допущено до захисту
«___» _____ року

Студента групи М 01-18
факультету економіки і права
освітньо-професійної програми
Управління та адміністрування
бізнес-процесами
спеціальності 073 Менеджмент
Євченко Олексія Євгеновича

Завідувач кафедри
менеджменту і маркетингу
_____Смагін В.Л.
(підпис)

Науковий керівник:
доктор економічних наук,
завідуючий кафедри
Смагін В.Л.

Національна шкала _____
Кількість балів _____
Оцінка ЄКТС _____

КИЇВ – 2019

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЛІНГВІСТИЧНИЙ УНІВЕРСИТЕТ

(повне найменування вищого навчального закладу)

Факультет, відділення ЕКОНОМІКИ І ПРАВА

Кафедра менеджменту і маркетингу

Ступінь вищої освіти МАГІСТР

Напрям підготовки Управління та адміністрування бізнес-процесами

(шифр і назва)

Спеціальність 073 МЕНЕДЖМЕНТ

ЗАТВЕРДЖУЮ
Завідувач кафедри
менеджменту і маркетингу
_____В.Л.Смагін
"30"листопада 2018 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Євченко Олексію Євгеновичу

1.Тема роботи «Інформаційна безпека бізнесу сучасної організації » (на прикладі ТОВ «ІНКОМ-ІНВЕСТ»)
керівник роботи Смагін Володимир Леонтійович, професор, доктор економічних наук
затверджені наказом Київського національного лінгвістичного університету від «6» листопада 2018 року №1263-с

2.Строк подання студентом роботи 21 листопада 2019 року
3.Вихідні дані до роботи: мета роботи полягає в розробці шляхів вдосконалення інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ»; об'єктом дослідження є господарські операції та процеси пов'язані з удосконаленням системи інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ»;предметом дослідження є інформаційна безпека бізнесу на сучасному підприємстві.
4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Обгрунтувати теоретико-методологічні основи інформаційної безпеки бізнесу. 2. Надати загальну характеристику діяльності та зовнішнього середовища ТОВ «ІНКОМ-ІНВЕСТ». 3.Запропонувати елементи покращення інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ».
5. Дата видачі завдання 30 листопада 2018 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	**Назва етапів виконання кваліфікаційної роботи магістра**	**Строк виконання етапів**
1.	Затвердження теми кваліфікаційної роботи	06.11.2018
2.	Затвердження завдання на кваліфікаційну роботу і плану кваліфікаційної роботи	до 30.11.2018
3.	Підготовка і подання науковому керівнику вступу та І-го розділу кваліфікаційної роботи	до 28.05.2019
4.	Підготовка і подання науковому керівнику ІІ-го розділу кваліфікаційної роботи	до 21.10.2019
5.	Підготовка і подання науковому керівнику ІІІ-го розділу кваліфікаційної роботи, висновків і резюме	до 06.11.2019
6.	Подання на кафедру остаточного тексту кваліфікаційної роботи в паперовому і електронному варіанті, заяви студента про допуск до захисту, висновку наукового керівника і відгуку від підприємства (організації) – бази дослідження	19.11.2019
7.	Попередній захист кваліфікаційних робіт на кафедрі та прийняття за результатами перевірки робіт рішення про допуск їх до захисту у екзаменаційній комісії з атестації здобувачів ступеня вищої освіти «магістр»	21.11.2019
8.	Передавання кафедрою примірника кваліфікаційних робіт у паперовому і електронному варіанті у бібліотеку для внесення їх до репозитарію КНЛУ та подання примірника кваліфікаційних робіт разом із повним пакетом необхідних документів деканові факультету економіки і права	02.12.2019
9.	Захист кваліфікаційних робіт в екзаменаційній комісії з атестації здобувачів ступеня вищої освіти «магістр»	16.12.2019–28.12.2019

ЗМІСТ

ВСТУП

Актуальність теми дослідження інформаційної безпеки полягає в тому, що в сучасному світі інтенсивно розвиваються інформаційні технології, що так само як глобалізація і становлення інформаційної економіки, відноситься до ряду макротенденцій сучасного світового правління.

За період свого існування, і особливо за останнє десятиліття, в сфері використання інформаційних технологій відбулися кардинальні зміни. Вони принесли бізнесу істотну вигоду, але при цьому потребували більш конкретної і серйозної уваги в сфері безпеки з сторони правління комерційного організації або фірми, інших організацій та приватних користувачів, котрі розробляють інформаційні системи, надають їх в користування, обслуговують або використовують їх.

Інформаційні ризики реалізуються через вразливість сучасних інформаційних систем, підтримуючих різні види господарської діяльності промислових та комерційних підприємств. В цій ситуації виникає необхідність забезпечення інформаційної безпеки соціально-економічної системи в цілому.

Тенденції розвитку промислових підприємств України показують, що керівництво вже приймає деякі міри захисту секретної або важливої інформації, однак ці дії не носять системного характеру, оскільки напрями на ліквідування певних загроз. Також однією з основних проблем промислових підприємств в цій сфері є відсутність затвердженої політики безпеки інформації.

Проблемами безпеки інформаційної безпеки на підприємствах України займались такі вітчизняні вчені як О.Курилко, О.Макаренко та В.Савелієв.

Мета роботи полягає в розробці шляхів вдосконалення інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ».

В роботі поставлено наступні завдання :

- визначити поняття інформаційної безпеки;
- дослідити принципи використання інформаційної безпеки на сучасному підприємстві;
- надати загальну системну характеристику підприємства;
- визначити слабкі місця інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ»;
- запроповати варінти вирішення проблем інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ».

Об’єктом дослідження є господарські операції та процеси пов’язані з удосконаленням системи інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ».

Предметом дослідження є інформаційна безпека бізнесу на сучасному підприємстві.

Методи дослідження: Теоретичною і методологічною основою проведених у роботі досліджень стали наукові концепції і теоретичні розробки провідних вітчизняних і зарубіжних вчених. У процесі досліджень застосовувались методи загальнонаукового пізнання економічних процесів, окрім цього використовувались методи теоретичного узагальнення та порівняння; статистичний аналіз; системний підхід.

Інформаційна база дослідження – періодичні публікації провідних вітчизняних та зарубіжних економістів, практиків управління персоналом, науково-теоретичні праці, монографії, підручники, посібники, статті у спеціальній фаховій періодиці, які забезпечили розкриття теоретико-методологічних основ інформаційної безпеки; нормативно-правові документи, що регулюють діяльність підприємств сфери послуг у сучасних вітчизняних соціально-економічних умовах; статистично-звітна документація бази дослідження ТОВ «ІНКОМ-ІНВЕСТ», організаційні та планові документи, на основі опрацювання яких здійснено аналіз інформаційної безпеки.

Практичне значення отриманих результатів полягає у виявленні, процесі дослідження емпіричної бази, недоліків в системі інформаційної безпеки, а також подолання їх за допомогою запропонованих заходів, а саме: аналіз шляхів ефективної політики ТОВ «ІНКОМ-ІНВЕСТ» та запропонуванні методичних рекомендацій щодо вдосконалення особливостей і умов використання систем інформаційної безпеки. Результати дослідження можуть бути використані у процесі подальшого удосконалення діяльності підприємств.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ БІЗНЕС-СЕРЕДОВИЩІ

1.1. Зміст та роль інформаційної безпеки, як специфічного виду діяльності.

Інформативна безпека підприємства - це положення безпеки корпоративних даних , при котрій гарантується їх секретність, цілісність, достовірність також загальнодоступність.

Інформативна безпека компанії досягається єдиним комплексом координаційних та промислових заходів, націлених на захист колективних відомостей. Координаційні заходи містять документовані процедури та принципи діяльність з різними типами даних, IT-сервісами, засобами безпеки також . Промислові заходи складаються у застосуванні апаратних та програмних засобів контролю допуску, прогнозу витоків, антивірусної безпеки, міжмережевого екранування.

Проблеми концепцій інформативною захищеності компанії різноманітні. Дане надання захищеного збереження даних в різних носіях; охорона відомостей, переданих каналами взаємозв'язку; розподіл допуску до різних типів документації; створення резервних копій, після-аварійне відновлення інформаційних .

Забезпечення інформативної захищеності компанії можливо тільки лише при системному підході та єдиному підході до безпеки. У концепції інформаційної безпеки повинні передбачатися всі без винятку важливі комп’ютеризовані небезпеки і також уразливості.

Повна інформативна захищеність компаній та установ передбачає постійний нагляд у цьому періоду абсолютно всіх значущих подій також станів, що впливають на недоторканність відомостей. Захист зобов'язаний реалізуватися цілодобово з її приходу або формування аж до знищення чи втрати актуальності.

Аспект до предметів вивчення так само як до концепцій висловлює одну з основних відмінних рис поточного академічного осягнення. З метою встановлення місця і ролі системи інформаційної безпеки (СІБ) у складі концепції управління підприємством, але крім того розкриття характерних рис впливу СІБ на систему виробництва також управління підприємством, проаналізуємо організацію зі позицій системного підходу.

Системний підхід - методика вивчення складних об’єктів об’єднання елементів, пов'язаних комплексом взаємин один з одним. Головною проблемою системного підходу вважається поєднання, що містить планування концепцій також систему дій, спеціалізованих з метою звершення конкретних цілей також відповідних згідно оптимальному аспекту.

З середини минулого століття під впливом різних абстрактних підходів до управління системою (концепція прийняття висновків та кількісний підхід, комплексний також ситуативний підходи, теорії стратегії, інновацій і лідерства) склалися поняття про неї, так само як розкритою концепції в єдності умов внутрішньої також зовнішньої сфери, спрямованої в задоволеність покупців, в якої основним джерелом доходу є люди, що володіють знаннями.

В сучасній науці організація розглядається так само як відкрита, саморегулююча концепція, яка складається з підсистем та компонентів,

що взаємодіють між собою та зовнішньої сферою, в цілях отримання кінцевого продукту.

Внутрішня сфера компанії характеризується внутрішніми змінними, які у головному вважаються підсумком адміністративних рішень. Це - місії, склад, проблеми, технологічні процеси та суспільство. Зовнішня інформативна сфера компанії поділяється на сферу безпосереднього впливу та непрямого впливу, характеризується складністю, рухливістю та невизначеністю.

Початковим ланкою системи вважається елемент, що відображає собою предмет, який не поступається подальшого поділу в частки. Елементи можуть розглядатися так само як елементарні системи, які у даному взаємозв’язку і на даному рівні дослідження не поділяють на підсистеми. Елементами можуть бути не тільки матеріальні об’єкти, а і виробничі процеси, функції. З метою постанови покладених на організація задач воно здійснює самоорганізацію та акцентує у своєму складі підсистеми, у рамках яких, виконуються конкретні види діяльності.

Крім цього, підприємство розглядається як система процесів, що показують собою комплекс дій, націлених на перенаправлення ресурсів в підсумках (продукт, послуга). При самому загальному підході всі без винятку основні процеси компанії можливо розбити в інформаційні процеси та процеси, що носять матеріальний вид. Інший підхід до систематизації дій грунтується в їх значущості у формуванні нових цінностей, у відповідності зі ним, виділяють наступні процеси:

1) основні (пов'язані з виробництвом та забезпечують життєвий процес компанії);

2) забезпечуючі (опорні основні процеси з позиції їх безперервності та економічності);

3) адміністративні (створюють вимоги та використовують умови, необхідні з метою звершення цілей компанії) .

Є велика кількість систематизаційних компонентів та підсистем компанії згідно з різними критеріями. Таким чином, відштовхуючись від класифікації , відповідно до змісту, у виробничій концепції компанії можна відзначити відповідні підсистеми:

1) соціальну (сукупність взаємовідносин між людьми);

2) виробничо-технічну (Матеріальні ресурси: комплекс машин та обладнання, матеріалів, інструментів);

3) інформаційну(інформаційні компоненти та їх взаємозв'язку).

Суть функціонування системи в цьому випадку зводиться до переміщенню інформації, використаних матеріалів, пов'язаного з переробкою конкретної вхідної інформації (наприклад, використані матеріали, відомості, прилади, економічні ресурси). Наукою про організацію виробництва організація розглядається в комплексі, в зв'язку абсолютно всіх аспектів. В якості предмета цього дослідження виступає інформаційна захищеність, що розглядається також так само як сфера академічних досліджень, так само як область фактичної роботи. Під інформаційною безпекою мається на увазі «стан безпеки інформативної сфери організації, що забезпечує її розвиток, застосування та формування у інтересах людей, установ, держави».

Інформаційна безпека вважається один з основних нюансів загальної безпеки, на якому б рівні ми її не аналізували - державному,

галузевому, колективному або індивідуальному. У цьому випадку інформаційна захищеність розглядають в колективному ступені, так як система вступає у єдину концепцію захищеності компанії. В той самий час сама інформаційна безпека може розглядатись як система і структурно включать в себе наступні підсистеми:

- координаційно-правову захищеність даних;
- інженерно-технічний захист даних;
- програмно-апаратний захист даних;
- фізичний захист даних;
- захист інформації в мережі та системах.

Необхідність використання системного підходу до компанії інформаційної безпеки підприємницької діяльності пов'язана з тим, то що захист даних вважається головною та єдиною складовою єдиної системи надання безпеки даної діяльності, в тому числі у фінансових, суспільно-політичних, громадських, а також інших аспектах. В першу чергу, необхідно розуміти, що безпека даних має незалежне значення лише відносно, оскільки вона має забезпечити ефективне функціонування економічної системи (підприємства), і тому охоплює та залучає в свою сферу різні елементі, зв’язаними не випадковими, а стійкими, впливаючими один на одного і залежними один від одного зв’язками.

Зрозуміти абсолютно всю різноманітність даних взаємозв'язків можливо тоді, коли застосовується системний підхід в організації інформаційної безпеки підприємницької діяльності.

Будь-яка система захисту інформації має свої особливості і в той же час повинна відповідати єдиних умов, з числа яких, акцентуються наступні:

- концепція захисту інформації зобов'язана бути показана як щось єдине. Єдність концепції стане проявлятися у присутності загальної місії її функціонування, інформативних взаємозв'язків між елементами системи, ієрархічності побудови підсистеми управління системою захисту інформації.
- концепція захисту інформації зобов'язана гарантувати безпеку інформації, грошей даних також захист інтересів учасників інформаційних взаємин.
- концепція захисту інформації в цілому, методи та засоби захисту не повинні формувати додаткових незручностей працівникам, та в той же час бути важкодоступними для несанкціонованого доступу зловмисників до захищеної інформації.
- концепція захисту інформації повинна забезпечувати інформаційні взаємозв'язки зсередини системи між її елементами для узгодженого їх функціонування і зв’язку з зовнішнім середовищем, перед котрим система проявляє свою цілісність і виступає як єдине ціле.

Система захисту інформації містить у собі комплекс компонентів, які її утворюють, та ті що надають їй певні властивості. Внутрішні взаємозв'язки системи та їх властивості створюють архітектурну систему, її структуру та внутрішню організацію. Водночас елементи системи мають зовнішні взаємозв'язки, які навмисно впливають на зовнішню сферу та вирішують поставлені перед системою задачі, це - багатофункціональна частка системи. Безумовно, те що обидві частини

системи - структурна та багатофункціональна - ніяк не відокремлені один від одного.

Структурна частина системи захисту інформації є її внутрішня організація, що дає можливість системі відповідно до норми працювати, формує вимоги з метою надання захищеності конфіденційної інформації, її обробка та використання тільки згідно каналів, регульованими цією системою.

1.2.Види загроз для інформаційної безпеки бізнесу в умовах діяльності організації

В наш час в діяльності будь-якого комерційного підприємства досить значну значимість має захист інформації. Інформація на сьогоднішній день - цінне джерело, від якого залежить як діяльність компанії в цілому, так і його конкурентоспроможність.

Загрозами безпеки інформаційних ресурсів компанії велика кількість - це комп'ютерні віруси, які можуть ліквідувати важливі дані, та промислове шпигунство зі сторони конкурентів котрі переслідують мету отримання протизаконним шляхом доступу до даних що представляють комерційну таємницю, також велика кількість інших загроз.

Тому особливу роль виконує робота по захисту інформації, згідно забезпеченню інформативною захищеності.

Інформаційна безпека - безпека даних та інформації та належної інфраструктури з несподіваних або навмисних впливів супроводжуваних нанесенням шкоди власникам і користувачам даних.

Інформативна захищеність - надання конфіденційності, цілісності та доступності даних.

Завдання захисту інформації і її даних - мінімізація витрат, стимульованих порушенням цілісності або конфіденційності даних, і також їх недоступності для споживачів.

Головні види загроз інформаційної безпеки:

- загрози конфіденційності - несакціонований доступ до даних (наприклад, отримання сторонніми особами інформації про стан рахунків клієнтів банку, домашня адреса клієнта або його контактні дані).
- загрози цілісності - несанкціоноване оновлення, доповнення, зміни або видалення даних (наприклад, внесення змін у бухгалтерські проводки з ціллю розкрадання грошових коштів).
- загрози доступності - лімітування або блокування доступу до даних (наприклад, не можливість підключення до сервера з базою даних в слідстві DDoS-атаки).

Список джерел небезпеки:

1. Внутрішні:

- помилки користувачів та адміністраторів;
- помилки в роботі програмного забезпечення;
- перебої в роботі комп'ютерного оснащення;
- недотримання працівниками фірми регламентів по роботі з інформацією.

2. Зовнішні небезпеки:

- несанкціонований доступ до інформації зі сторони зацікавлених установ, організацій та окремих осіб (промислове шпигунство конкурентів, отримання даних спецслужбами, атаки хакерів);
- комп’ютерні віруси та інші шкідливі програми;
- стихійні лиха та техногенні катастрофи (наприклад, шторм здатний призупинити службу телекомунікаційної сітки, або пожежа

може ліквідувати або пошкодити сервери з важливою інформацією).

Способи надання захищеності даних в інформаційній мережі:

• Перешкоджання - фізичне перешкоджання шляху правопорушника до інформації, що захищаються (наприклад, комерційно важлива інформація знаходиться на сервері всередині будівлі фірми, допуск до якої володіють тільки її працівники).

• Керівництво доступом - врегулювання застосування інформації та допуску до неї через систему ідентифікації користувачів, їх розпізнавання, перевірка повноважень та рівнів доступу (наприклад, якщо допуск у відділення або на поверх з комп’ютерним обладнанням, в яких, знаходиться засекречена інформація, можливий тільки за наявністю особливої картці-пропуску.

Або якщо будь-якому працівнику виділяється індивідуальний логіну та паролю з метою допуску до бази даних компанії з різними ступенями доступу) .

• Криптографія - кодування інформації з підтримкою спеціалізованих алгоритмів (наприклад, кодування інформації пересиланню їх пересилання через мережу Інтернет; або застосування електронного-цифрового підпису).

• Опір атакам шкідливих програм - мається на увазі застосування зовнішніх накопичувачів даних тільки з перевірених джерел, антивірусних програм, брандмауерів, систематичне виконання додаткового резервного копіювання важливих даних (шкідливих програм досить велика кількість вони також поділяються на кілька видів: віруси, логічні бомби, трояни, мережеві черв'яки).

• Регламентація - формування вимог згідно з обробкою, передачі та збереженню інформації, на найвищому ступені забезпечуючих її захист (спеціалізовані норми та стандарти для персоналу по роботі з даними, наприклад, створення резервних копій всієї інформації з певною періодичністю, котрі забороняють використання власних зовнішніх інформаційних накопичувачів.).

• Зобов'язання - формування правил по роботі з інформацією, недотримання яких, карається матеріальною, адміністративною або кримінальною відповідальністю (штрафи, Закон України «Про охорону прав на комерційну таємницю»[20]).

• Мотивування - заклик до персоналу не порушувати встановлені порядки по роботі з комерційною або секретною інформацією, котре суперечить сформованим моральним нормам (наприклад, Кодекс професійної поведінки членів «Асоціації користувачів електронно-обчислювальних машина США»[2]).

Засоби захисту інформації:

• Технічні (апаратні) ресурси - сигналізація, генератори перешкод для передачі даних або інформації по радіоканалах, електронним джерела.

• Програмні засоби - програми-шифрування інформації, антивіруси, системи аутентифікації користувачів.

• Гібридні ресурси - поєднання технічних та програмних ресурсів.

• Організаційні засоби - принципи роботи, регламенти, законодавчі акти у галузі захисту інформації, підготовка приміщень з комп'ютерною технікою та прокладка мережевих кабелів з урахуванням вимог по обмеженні доступу до інформації.

1.3 Організація інформаційної безпеки у підприємницьких організаціях

На даний період актуальна та об'єктивна інформація вважається значущим фактором виробництва, що оцінюють як один з ключових ресурсів формування спільноти. Інноваційні інформативні концепції та технологічні процеси вважаються знаряддям збільшення продуктивності та продуктивності діяльність працівників.

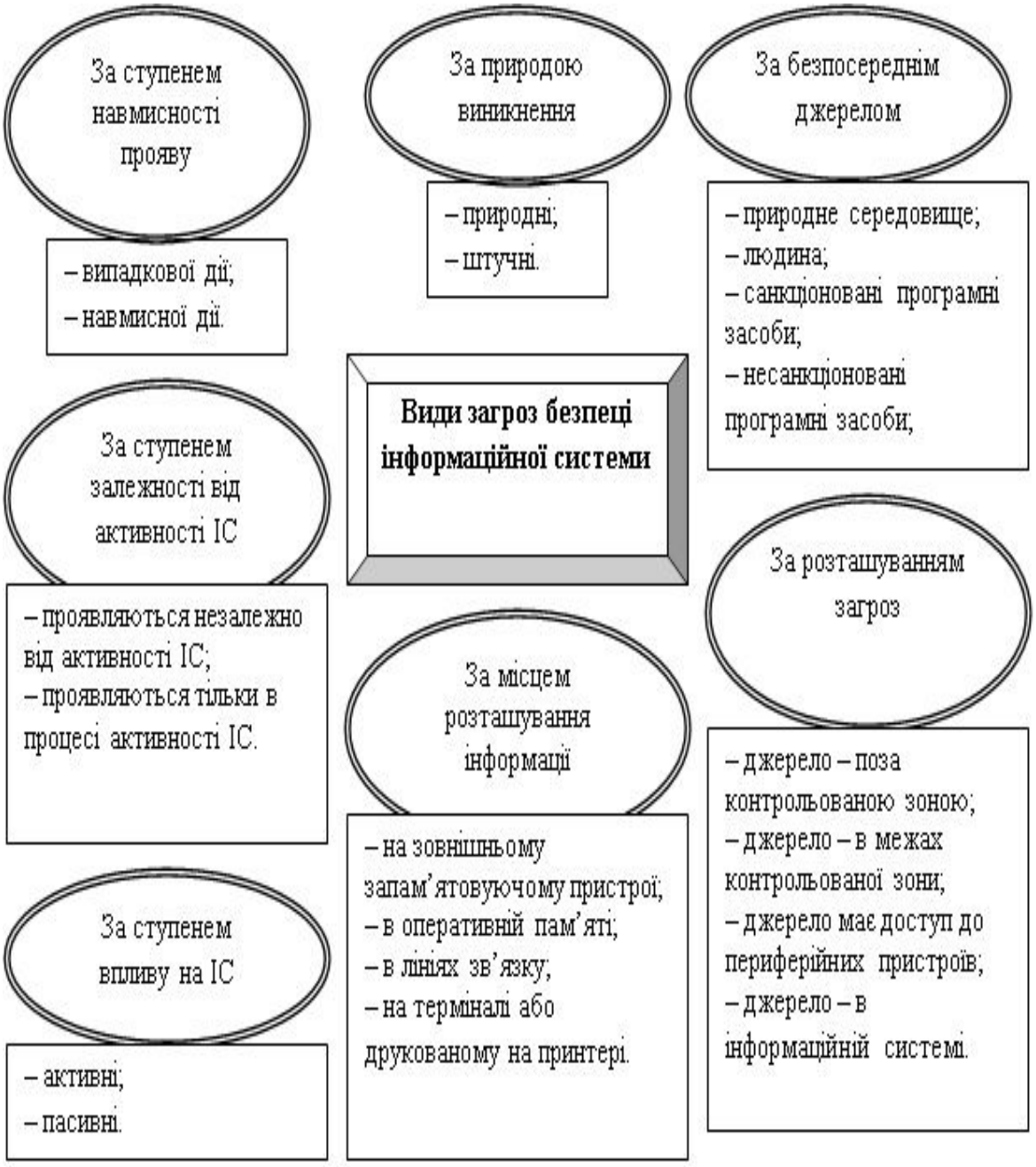
Але світовий досвід комп'ютеризації в безлічі областях управління та виробництва супроводжується виникненням новітніх небезпек інтересів підприємницької діяльності, суспільства, країни .

Одночасно з формуванням та ускладненням засобів, способів, конфігурацій форм автоматизації дій оброблення даних збільшується взаємозалежність суб'єктів підприємництва з рівня захищеності застосовуваними інформаційними технологіями[35].

Можливо визначити кілька ключових небезпек інформаційної безпеки сучасної компанії:

- незаконна діяльність певних фінансових та економічних структур в області розвитку, поширення та застосування інформації;
- недотримання встановлення регламентів збору, оброблення та передачі інформації;
- навмисні та випадкові дії персоналу працюючих в сфері або підрозділах інформаційних систем;
- похибки у конструюванні інформаційних систем;
- несправність технічних засобів та перебої в роботі програмного забезпечення в інформаційних та телекомунікаційних системах тощо. [35].

На даний період експертами вивчається досить великий список небезпек захищеності інформаційних систем [11], які систематизують відповідно до певних властивостей (Рис 1.1).



Захист інформації - сфера науки та технічних досліджень, що активно розвивається, дає ринку великий діапазон ресурсів та засобів з

метою захисту інформації. Але кожен з них окремо обраний не в силах забезпечувати відповідну захищеність інформативної системи. Важливою обставиною результативної безпеки вважається проведення комплексу щодо захисту даних [4].

Комплексне надання інформаційної безпеки автоматизованих систем - це комплекс шифрувальних, програмно-апаратних, промислових, законних, правових, координаційних засобів та забезпечення безпеки інформації при її обробленню, збереженні та передачі з застосуванням нинішніх комп'ютерний технологій [11].

З липня 2003 у Україні впроваджена кримінальна відповідальність через протизаконне вторгнення в роботу комп'ютерних систем та комп'ютерних мереж, але крім того за поширення комп'ютерних вірусів та програм що вносять інформаційні зміни до носіїв інформації, т що призводить до зникнення, блокування даних або її носіїв [4].

Досвід демонструє, те що майже будь-яка організація має противірусні засоби безпеки, системи ідентифікації користувачів, системи управління допуском до інформативної бази. Тобто можливості розвитку та реалізації безпеки є, однак фірми ніяк не реалізують його цілком. Більш того, володіючи спецалізованим апаратними забезпеченням захисту інформації , велика частина компаній не використовую свої ресурси навіть на половину потужності задля забезпечення потрібного рівня інформаційної безпеки. Переважно більша частина умов стандартів інформаційної захищеності можуть бути виконані існуючими можливостями компаніями для безпеки [53].

Сучасна комерційна організація зобов'язана мати здатність належним чином створювати політику інформаційної захищеності, тобто створювати та результативно запроваджувати сукупність

попереджувальних заходів згідно безпеки секретних відомостей та інформаційних процесів. Подібна стратегія передбачає належні вимоги до персоналу,менеджерів та технічних служб [11].

Основними стадіями побудови політики інформаційної захищеності вважаються:

- реєстрування всіх ресурсів, які мають бути захищені;
- дослідження та формування переліку можливих небезпек для будь-якого ресурсу;
- аналіз ймовірності виникнення будь-якої загрози;
- прийняття мір, які дають можливість економічно та результативно захистити інформаційну систему [4].

Велика частина експертів у сфері інформаційної безпеки вважають, те що інформаційна захищеність утримується на належному рівні, в разі якщо для абсолютно всіх інформаційних ресурсів системи утримується відповідний ступінь конфіденційності (несанкціонованого отримання будь-якої інформації), цілісності(несанкціонованого, навмисного або несподіваного оновлення даних) та доступності (здатності негайно отримати запитувану інформацію) [11].

Можна визначити відповідні підсистеми результативного захисту даних в компанії:

- Підсистема противірусної безпеки шлюзів входу в мережу Інтернет, файлових серверів, центрального управління, періодичного оновлення противірусних баз даних.
- Підсистема управління контролем доступу та ідентифікацією в системі інформаційної безпеки.

- Підсистема міжмережевого екранування, що дає можливість здійснити захищеність міжмережевого каналу через взаємодії за допомогою застосування програмних та програмно-апаратних міжмережевих екранів.
- Підсистема шифрувальної безпеки, що забезпечує захищеність з'єднання завдяки шифрування даних.
- Підсистема захисту від інсайдерів, що здійснює контроль дії порушників, здійснить інформаційну безпеку при управлінні допуском та реєстрації.
- Підсистема захисту концепцій управління базами даних.
- Підсистема виявлення вторгнень та зусиль несанкціонованого допуску до інформаційних ресурсів компанії. Система гарантує реалізацію запобіжних подій згідно протидії атакам хакерів та поширенню спам-матеріалу.
- Підсистема захисту мобільних приладів.
- Підсистема прогнозу подій інформаційної безпеки, що дає можливість вчасно виявляти небезпеки інформативною концепції та негайно реагувати на них [53].

На сьогоднішній день спеціалізовані підприємства дають великий діапазон послуг систем інформаційної безпеки з урахуванням їх ціни та функціональних можливостей. Більш прийнятним підходом при підборі цього або іншого виду вважається виконання принципу «розумної достатності», сутність якого полягає в тому, що характерними при конструюванні політики інформаційної безпеки зобов'язані бути: розмір компанії, його ресурсні та економічні можливості, справжній ступінь інформативної захищеності.

Безперервна діяльність у галузі підтримки інформаційної безпеки в належному ступені вважається важливою обставиною продуктивності підприємницької роботи .

В той самий час система інформаційної безпеки має бути розглянута як важлива складова загальної безпеки підприємства. При цьому потрібно створювати концепції інформаційної безпеки, дивлячись на котру треба передбачити не лише заходи, котрі взаємопов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та аутентифікації.) , але і належні заходи управлінського та технологічного характеру [22].

Одним елементів організації інформаційної безпеки є розробка політики інформаційної безпеки.

У базі координаційних заходів захисту даних знаходиться стратегія захищеності, від продуктивності якої в максимальному ступені залежить успішність подій по забезпеченню інформативною захищеності.

Під розумінням політики інформативної безпеки мається на увазі комплекс документованих адміністративних висновків, націлених на захист інформаційних ресурсів компанії. Це дає можливість забезпечити результативне керівництво та підтримати політику в сфері інформативною захищеності зі сторони управління компанії.

Стратегія захищеності будується на основі розгляду ризиків. З урахуванням ризиків, виявлених в компанії, політика інформаційної безпеки для підприємства повинна включати 5 розділів:

- «Вступ». Потреба виникнення політики безпеки в основі виявлених недоліків в інформаційній захищеності компанії;

- «Мета політики». У даній розділі важливого документа для підприємства слід відобразити цілі формування цього важливого документа;
- «Галузь застосування». У цьому розділі слід викласти суб'єкти компанії, які зобов'язані виконувати умови цієї політики ;
- «Політика». У цьому області слід викласти самі вимоги до інформаційної безпеки (наприклад, парольна стратегія повинна включати 5 підрозділів: «Створення паролів», «Зміна паролів», «Захист паролів», «Використання паролів при розробці додатків», «Використання паролів при віддаленому доступі »);
- «Відповідальність». Описує санкцію через недотримання зазначених у минулому розділі умов;

Подібна структура дасть можливість коротко викласти всі основні нюанси, пов'язані з об'єктом політики безпеки компанії, не "прив'язуючись» до конкретних технологічних рішень, продуктам та виробникам. Інакше зміни політичної ситуації в компанії може призвести до необхідності зміни концепції ІБ, але цього відбуватись не повинно.

Крім цього, в політиці безпеки компанії мають бути встановлені прямі обов'язки посадових осіб відповідно до вироблених норм безпеки.

РОЗДІЛ 2. Характеристика підприємства ТОВ «ІНКОМ-ІНВЕСТ»

2.1 Загальна характеристика підприємства ТОВ «ІНКОМ-ІНВЕСТ»

За час роботи на ринку нерухомості Києва компанія ТОВ «ІНКОМ-ІНВЕСТ» зуміла проявити себе, як команда однодумців орієнтованих на результат. Накопичений досвід і знання спільно з цілеспрямованістю і високим професіоналізмом співробітників дозволяє проводити операції з оформлення угод будь-якої складності і в оптимальні терміни для замовника. Компанія ТОВ «ІНКОМ-ІНВЕСТ» веде свою діяльність на ринку нерухомості ось уже понад 17 років.

Таблиця 2.1

Загальна інформація про підприємство ТОВ «ІНКОМ-ІНВЕСТ»

Повне найменування юридичної особи	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ ІНКОМ-ІНВЕСТ
Скорочена назва	ТОВ ІНКОМ-ІНВЕСТ
Статус юридичної особи (Станом на 03.10.2019)	Не перебуває в процесі припинення
Код ЄДРПОУ	32068777
дата реєстрації	04.07.2002 (17 років 2 місяці)
Уповноважена особа	ВЕРЕМІЄНКО ОЛЕКСАНДР КОСТЯНТИНОВИЧ
Організаційно-правова форма	Товариство з обмеженою відповідальністю
Форма власності	недержавна власність
Види діяльності	Основний: 68.20 Оренда і управління власною або орендованої нерухомістю
	інші: 61.10 Кабельна телекомунікаційна зв’язок 68.10 Купівля та продаж нерухомості

	68.32 Управління нерухомістю за винагороду або на договірній основі
Адреса	03057, м. Київ, Соломянський район, вул.. Смоленська, буд. 31-33

Аналіз діяльності підприємства проведемо на основі дослідження таких груп показників, як: оцінки фінансових результатів, рентабельності, фінансової стійкості, ліквідності, ділової активності.

Таблиця 2.2

Динаміка фінансових результатів ТОВ «ІНКОМ-ІНВЕСТ»

в 2016-2018 рр.

Показники	Роки, тис. грн.			Абсолютний приріст		Темп приросту, %	
	2016	2017	2018	2017-2016	2018-2017	2017/2016	2018/2017
Чистий дохід (виручка) від реалізації послуг	4335,5	5722	7002,1	1386,5	1280,1	31,98	22,37
Інші доходи	144,7	157,4	216,2	12,7	58,8	8,78	37,36
Валовий прибуток	1317	1377,5	1753,8	60,5	376,3	4,59	27,32
Разом чисті доходи	4480	5879,4	7228,5	1399,4	1349,1	31,24	22,95
Собівартість реалізованої послуг	3018,5	4344,5	5248,3	1326	903,8	43,93	20,80
Інші операційні витрати	948,7	1201,5	1535,3	252,8	333,8	26,65	27,78
Разом витрати	3967,2	5546	6783,6	1578,8	1237,6	39,80	22,32
Фінансовий результат до оподаткування: прибуток	512,8	333,4	444,9	-179,4	111,5	-34,98	33,44
Витрати з податку на прибуток	80,3	60	80,1	-20,3	20,1	-25,28	33,50
Чистий фінансовий	432,5	273,4	364,8	-159,1	91,4	-36,79	33,43

результат: прибуток							

За даними табл. 2.2 можемо зробити висновок, що протягом 2016-2018 рр. чистий дохід підприємства мав чітку динаміку до зростання на 31,98% в 2017 році та на 22,37% за результатом 2018 року і становив відповідно 5722 тис. грн. в 2017 році та 7002,1 тис. грн. за результатом 2018 року.

Слід відмітити, що сумарні доходи підприємства мали аналогічну динаміку до зростання на 31,24% за результатом 2017 року та на 22,95% за результатом 2018 року і становили 5879,4 тис. грн. та 7228,5 тис. грн. відповідно.

Чистий прибуток підприємства протягом 2017 року зменшився на 36,79% до рівня 273,4 тис. грн., а за результатом 2018 року зросли на 33,43% до рівня 364,8 тис. грн.(рис. 2.1)

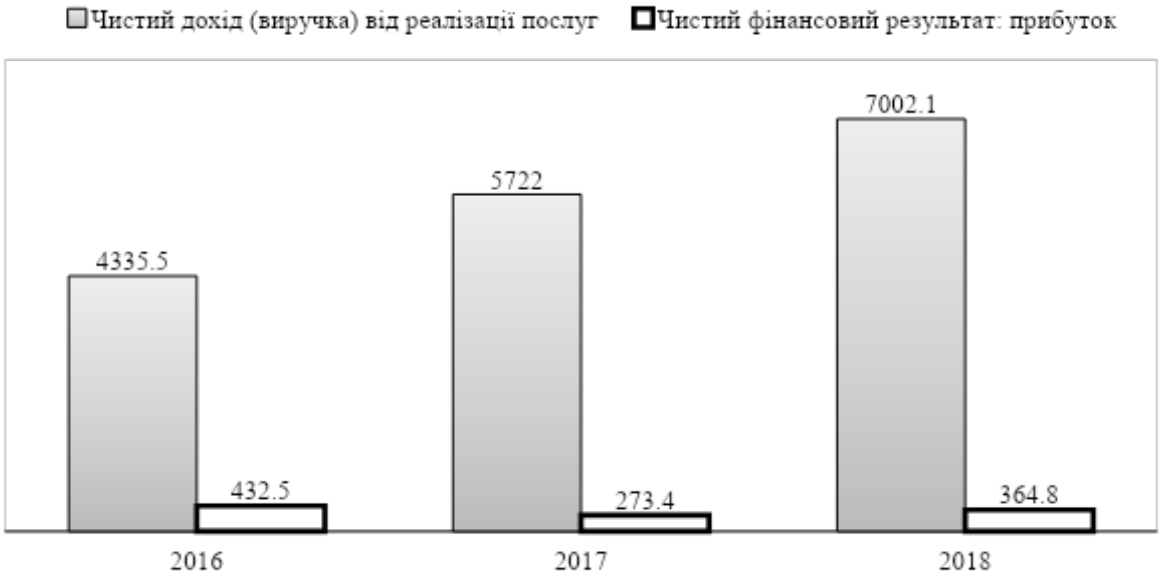


Рис. 2.1. Динаміка чистого доходу та чистого прибутку ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Коефіцієнт рентабельності діяльності розраховується як відношення чистого прибутку підприємства до чистої виручки від реалізації послуг. Збільшення цього показника свідчить про зростання ефективності господарської діяльності підприємства, а зменшення навпаки (табл. 2.3).

Таблиця 2.3

Динаміка показників рентабельності ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Показник	Роки			Абсолютне відхилення	
	2016	2017	2018	2017-2016	2018-2017
Рентабельність послуг, %	43,631	24,838	25,854	-18,793	1,016
Рентабельність основної діяльності, %	23,982	11,940	13,653	-12,042	1,713
Рентабельність сукупного капіталу, %	23,982	11,940	13,653	-12,042	1,713
Рентабельність власного капіталу, %	28,833	15,378	17,025	-13,456	1,648
Рентабельність операційних витрат, %	66,505	71,924	51,880	5,419	-20,045
Рентабельність операційного прибутку	83,338	72,751	63,088	-10,587	-9,663

Рентабельність діяльності по підприємству зменшилася у 2017 р. порівняно з 2016 р. на 12,04% і склав 11,94%. Зниження рентабельності основної діяльності пов'язана з тим, що у 2017 р. значно зросли загальні витрати. В 2018 році даний показник збільшився на 1,713% і становив 13,66%(рис. 2.2).

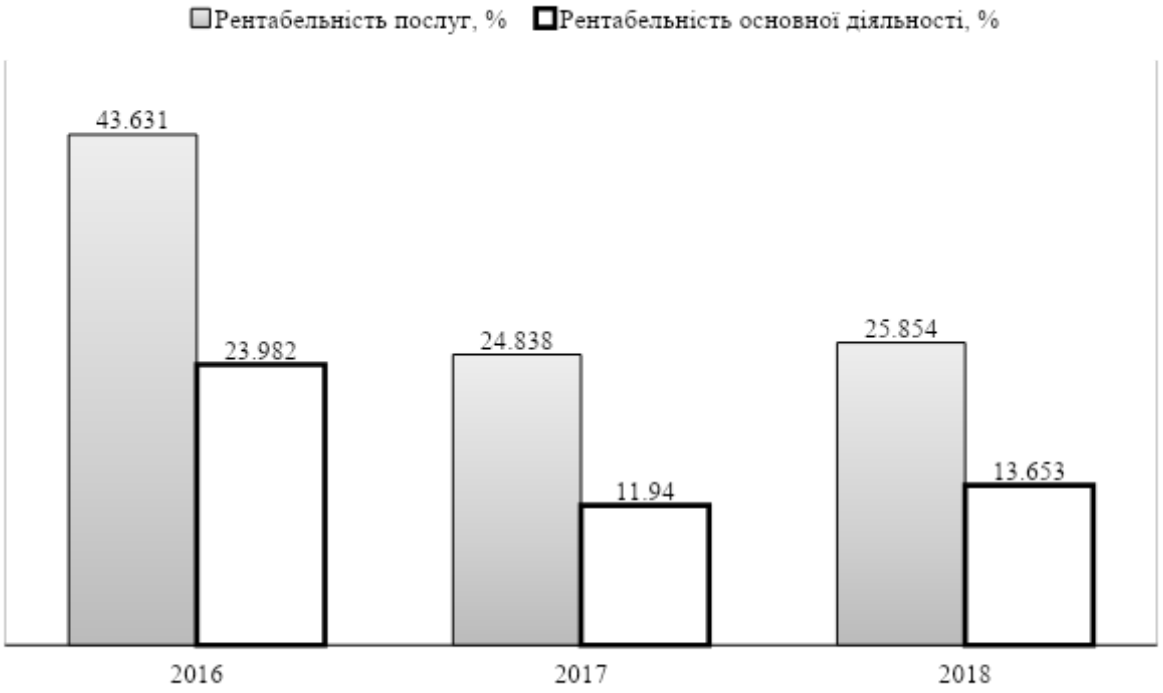


Рис. 2.2. Динаміка рентабельності послуг та основної діяльності ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Коефіцієнт рентабельності власного капіталу (фінансова рентабельність) характеризує рівень прибутковості власного капіталу, вкладеного в дане підприємство, тому найбільший інтерес представляє для наявних і потенційних власників й акціонерів й є одним з основних показників інвестиційної привабливості підприємства, тому що його рівень показує верхню межу дивідендних виплат.

Рентабельність власного капіталу 2016 році становив 28,83%, а в 2017 році, зменшившись на 13,456%, становив 15,378%. В 2018 році даний показник знову зріс – на +1,648%, і становив, таким чином, 17,025%.

Рентабельність послуг – характеризує вигідність виробництва послуг, яка випускається або реалізується підприємством; цей показник використовується при внутрішньогосподарських аналітичних

розрахунках, при контролі прибутковості, при впровадженні нових видів послуг. Рентабельність послуг підприємства в 2017 році становила 24,84% (сам показник зменшився на 18,79%), а в 2018 році показник зріс до рівня 25,85% (+1,016%). Динаміка даного показника свідчить про зростання ефективності та вигідності послуг, що здійснює підприємство.

Коефіцієнт оборотності основних засобів (фондовіддача) розраховується як відношення чистої виручки від реалізації послуг до середньорічної вартості основних засобів. Він показує ефективність використання основних засобів підприємства. Динаміка даного показника свідчить про зростання суми отриманих коштів підприємства на 1 грн. вкладених основних засобів: в 2017 році – 0,4,95 грн. до рівня 18,31 грн., в 2018 році – 4,98 грн. до рівня 23,29 грн. (табл. 2.4).

Таблиця 2.4

Динаміка показників ефективності використання основних засобів ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Показники	Роки			Абсолютний приріст	
	2016	2017	2018	2017-2016	2018-2017
Фондовіддача	13,36	18,31	23,29	4,95	4,98
Фондомісткість	0,07	0,05	0,04	-0,02	-0,01

Фондомісткість протягом досліджуваного періоду мала динаміку щодо зменшення, адже в 2017 році зменшення показника становило 0,02, а в 2018 році – 0,01 і становив він відповідно 0,05 грн. та 0,04 грн.

Коефіцієнт оборотності оборотних засобів в 2017 році зменшився на 0,38, а в 2018 році – зріс на 0,59 до рівня 29,53. Збільшення цього коефіцієнта свідчить про зростання обороту оборотних засобів. Зменшення показника тривалості обороту оборотних засобів в 2018 році

на 0,25 є позитивною динамікою, адже свідчить про зменшення кількості днів, протягом якого оборотні засоби проходять усі стадії одного кругообігу (рис. 2.3 та табл. 2.5).

Рис. 2.3. Динаміка коефіцієнту оборотності оборотних засобів ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Коефіцієнт оборотності дебіторської заборгованості протягом дослідженого періоду мав динаміку до зменшення, що є досить негативним явищем, адже зменшується кількість оборотів, яку здійснює дебіторська заборгованість протягом звітного періоду. В 2016 році даний показник становив 367,4, а в 2017 році при зменшенні в 233,4 склав 134. В 2018 році зменшення даного показника становило 30,58 і становив 103,4.

Рис. 2.4. Динаміка коефіцієнту оборотності дебіторської та кредиторської заборгованості ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Коефіцієнт оборотності кредиторської заборгованості в 2017 році становив 16,31, що більше за попередній період на 1,71. В 2018 році даний показник зменшився на 2,21 і склав 14,1. Отже, за період дослідження даний коефіцієнт мав динаміку до зменшення, що свідчить про зменшення кількості оборотів, яку здійснює кредиторська заборгованість протягом звітного періоду.

Таблиця 2.5

Динаміка показників ділової активності ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Показники	Роки			Абсолютний приріст	
	2016	2017	2018	2017-2016	2018-2017
Коефіцієнт оборотності оборотних засобів	29,32	28,94	29,53	-0,38	0,59
Тривалість обороту оборотних засобів	12,28	12,44	12,19	0,16	-0,25
Коефіцієнт оборотності дебіторської заборгованості	367,42	134,00	103,43	-233,41	-30,58
Тривалість обороту дебіторської заборгованості	0,98	2,69	3,48	1,71	0,79
Коефіцієнт оборотності кредиторської заборгованості	15,34	16,31	14,10	0,97	-2,21
Тривалість обороту кредиторської заборгованості	23,47	22,07	25,54	-1,40	3,46
Тривалість операційного циклу	13,26	15,13	15,67	1,87	0,54

Протягом досліджуваного періоду тривалість операційного циклу зросла за результатом 2017 року на 1,87 днів та за результатом 2018 року на 0,54 дні і становила відповідно 15,13 дня та 15,67 днів. Зростання даного показника за 2018 рік є негативним явищем, адже свідчить про зростання терміну перетворення дебіторської заборгованості на грошові кошти.

Коефіцієнт загальної ліквідності (коефіцієнт покриття) характеризує здатність підприємства забезпечити свої короткострокові зобов’язання з найбільше легко реалізованої частини активів – оборотних коштів. Цей коефіцієнт дає найбільш загальну оцінку

ліквідності активів. Протягом 2016-2017 рр. коефіцієнт покриття мав чітку динаміку до зменшення, при якій показник в 2016 році становив 4,874, в 2017 році – 3,863(зменшення на -1,011) (табл. 2.6).

Таблиця 2.6

Динаміка показників ліквідності ТОВ «ІНКОМ-ІНВЕСТ»
в 2016-2018 рр.

Показник	Роки			Абсолютне відхилення	
	2016	2017	2018	2017-2016	2018-2017
Коефіцієнт покриття (загальний коефіцієнт ліквідності)	4,874	3,863	4,481	-1,011	0,617
Коефіцієнт швидкої ліквідності	0,022	0,009	0,075	-0,013	0,065
Коефіцієнт абсолютної ліквідності	0,000	0,000	0,000	0,000	0,000
Коефіцієнт ліквідності запасів	4,791	3,766	4,287	-1,025	0,522
Коефіцієнт ліквідності коштів	0,022	0,009	0,075	-0,013	0,065

В 2018 році коефіцієнт покриття становив 4,481, що більше за попередній рік на 0,617. Динаміка коефіцієнту в 2018 році покриття свідчить про те, що підприємство збільшує обсяг оборотних коштів та зменшує борги, отже, може ліквідувати свої борги (рис. 2.5).

Коефіцієнт швидкої ліквідності розраховується як відношення найбільш ліквідних оборотних засобів (грошових засобів та їх еквівалентів, поточних фінансових інвестицій та дебіторської

заборгованості) до поточних зобов'язань підприємства. Він відображає платіжні можливості підприємства щодо сплати поточних зобов'язань за умови своєчасного проведення розрахунків з дебіторами.

Рис. 2.5. Динаміка коефіцієнту покриття ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Протягом 2016-2017 років коефіцієнт швидкої ліквідності мав динаміку до зменшення обсягів при якій показник в 2016 році становив 0,022, а в 2017 році – 0,09 (-0,013). В 2018 році відбулося зростання даного показника на 0,065 до рівня 0,075 (рис. 2.6).

Рис. 2.6. Динаміка коефіцієнту швидкої ліквідності ТОВ «ІНКОМ-ІНВЕСТ» в 2016-2018 рр.

Таким чином, протягом 2016-2018 рр. відбувалося зростання чистого доходу підприємства, що призвело до зростання чистого прибутку підприємства. Сумарні доходи підприємства мали аналогічну динаміку до зростання на 31,24% за результатом 2017 року та на 22,95% за результатом 2018 року і становили 5879,4 тис. грн. та 7228,5 тис. грн. відповідно. Рентабельність послуг підприємства в 2017 році становила 24,84% (сам показник зменшився на 18,79%), а в 2018 році показник зріс до рівня 25,85%(+1,016%). Динаміка даного показника свідчить про зростання ефективності та вигідності послуг, що здійснює підприємство. Динаміка коефіцієнту покриття в 2018 році свідчить про те, що підприємство збільшує обсяг оборотних коштів та зменшує борги, отже, може ліквідувати свої борги.

2.2 Інформаційна безпека бізнесу сучасної організації

Одна з основних внутрішньовиробничих функціональних складників безпеки підприємства – інформаційна. Вона полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Належні служби підприємства виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційного складника безпеки підприємства. До таких належать:

- збирання всіх видів інформації щодо діяльності того чи іншого суб'єкта господарювання;
- аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів;
- прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів;
- оцінка рівня економічної безпеки за всіма складниками та в цілому;
- розробка рекомендацій для підвищення цього рівня на конкретному суб'єктів господарювання;
- інші види діяльності з розробки інформаційного складника економічної безпеки.

На підприємство постійно надходять потоки інформації, що розрізняються за джерелами їхнього формування. Заведено відокремлювати:

1) відкриту офіційну інформацію;

2) вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації;

3) вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації.

Інформаційна безпека – стан захищеності основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну та телекомунікаційну інфраструктуру, власне інформацію та її параметри: повноту, об'єктивність, доступність і конфіденційність [33, с. 88].

Раціональним на наш погляд є визначення поняття «інформаційна безпека», як стану захищеності інформаційних відносин та пов'язаних із ними інформаційних процесів, за якого досягається стабільний інформаційний розвиток, унеможливлюється негативний інформаційний вплив та негативні наслідки незаконного застосування інформаційних технологій в усіх сферах суспільного життя, у результаті чого можна досягти створення та ефективного функціонування інформаційного суспільства [1].

Виходячи з вищенаведеного можна стверджувати, що інформаційну безпеку досліджують за такими основними характеристиками: стан захищеності інформаційного середовища та установлених законом правил, суспільні відносини. Розглянемо головні підходи до визначення поняття «інформаційна безпека підприємства», що існують сьогодні:

1) інформаційна безпека підприємства – це суспільні відносини щодо створення та підтримання на належному рівні життєдіяльності відповідної інформаційної системи [56];

2) інформаційна безпека підприємства – це суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [54];

3) інформаційна безпека підприємства – це відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів та дій уповноважених осіб, спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури даного підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях інформаційної системи підприємства [55, с. 5];

4) інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [37, с. 94].

Узагальнюючи перелічені та інші формулювання, на нашу думку, слід погодитись з визначенням Чередниченко А.О., що інформаційна безпека підприємства – це стан внутрішнього та зовнішнього інформаційно-комунікаційного середовища і процесів управління його складовими й діяльністю із забезпечення безпеки, що формує відповідний цілям функціонування підприємства рівень інформатизації і забезпечує попередження виникнення загроз інформаційній безпеці й нейтралізацію їх впливу [57, с. 7]. Оскільки об’єктом інформаційної безпеки підприємства є не окремий безпечний стан інформації, інформаційних ресурсів, інформаційної системи, інформаційного середовища, а його інформаційно-комунікаційне середовище.

Система управління інформаційною безпекою на ТОВ «ІНКОМ-ІНВЕСТ» є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної

безпеки. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Основними цілями інформаційної безпеки на підприємстві ТОВ «ІНКОМ-ІНВЕСТ» є:

- конфіденційність інформації, тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб;
- неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;
- цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), яка полягає в її існуванні в неспотвореному вигляді (незміненому по відношенню до деякому фіксованому її станом);
- доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до інформації, що їх цікавить;
- мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів;
- облік усіх процесів, пов'язаних з ризиками.

Досягнення заданих цілей на підприємства ТОВ «ІНКОМ-ІНВЕСТ» здійснюється в ході вирішення наступних завдань:

1. введення в систему термінів інформаційної безпеки;
2. класифікації інформаційних ресурсів підприємства;
3. визначення власників процесів, відповідальних за інформаційну безпеку;
4. розробки спектра ризиків інформаційної безпеки та проведення їх експертних оцінок;
5. визначення групи доступу до інформаційних ресурсів;

6. розробки системи управління ризиками інформаційної безпеки (методи та їх оцінка);

7. складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;

8. здійснення заходів інформаційної безпеки та періодичного контролю за станом ризиків;

9. забезпечення фізичної безпеки та безпеки персоналу;

10. розробки вимог до інформаційної системи з погляду інформаційної безпеки;

11. контролінгу інформаційної безпеки на підприємстві.

На ТОВ «ІНКОМ-ІНВЕСТ» виділяється чотири стадії реалізації системи управління інформаційною безпекою:

1) формування політики в галузі ризиків;

2) аналіз бізнес-процесів;

3) аналіз ризиків;

4) формування цільової концепції.

Загрози, з якими може зіткнутися ТОВ «ІНКОМ-ІНВЕСТ» класифікуються за природою їх виникнення, тобто загрози випадкового або навмисного характеру, і по тому, як вони ставляться до об’єкта захисту, тобто зовнішні і внутрішні загрози. Джерелами зовнішніх загроз ТОВ «ІНКОМ-ІНВЕСТ» є:

- діяльність конкурентів з перехоплення важливої інформації;
- навмисні дії з руйнування, знищення або модифікації інформації;
- ненавмисні дії співробітників сторонніх організацій, які потягли за собою відмову в роботі елементів системи;
- стихійні лиха та катастрофи, аварії, екстремальні ситуації.

До джерел внутрішніх загроз на ТОВ «ІНКОМ-ІНВЕСТ» відносяться:

- відсутність координації діяльності підрозділів підприємства у сфері захисту інформації;
- навмисні дії персоналу по знищенню або модифікації інформації;
- ненавмисні помилки персоналу, відмови технічних засобів і збої в інформаційних системах;
- порушення встановлених регламентів збору, накопичення, зберігання, обробки, перетворення, відображення та передачі інформації.

Порушення на ТОВ «ІНКОМ-ІНВЕСТ» можуть бути декількох видів. Організаційно-правові порушення - порушення, пов'язані з відсутністю єдиної узгодженої політики підприємства у сфері захисту інформації, невиконанням вимог нормативних документів, режимом доступу, зберігання та знищення інформації. Організаційні види порушень включають несанкціоноване отримання доступу до баз і масивам даних, несанкціонований доступ до активного мережевого обладнання, серверів, некоректне вбудовування засобів захисту і помилки в управлінні ними, порушення в адресності розсилки інформації при веденні інформаційного обміну. Під фізичними видами порушень мається на увазі пошкодження апаратних засобів автоматизованих систем, ліній зв'язку і комунікаційного устаткування, крадіжки або несанкціоноване ознайомлення зі змістом носіїв інформації, їх розкрадання. До радіоелектронних видів порушень відносяться впровадження електронних пристроїв перехоплення інформації, отримання інформації шляхом перехоплення і дешифрування інформаційних потоків, фотографування моніторів,

нав'язування неправдивої інформації в локальних обчислювальних мережах, передачі даних і лініях зв'язку. Для протидії загрозам і припинення порушень на підприємствах організовується процес управління ризиками, який є основою системи інформаційної безпеки підприємства.

Побудова ефективної системи інформаційної безпеки - це комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час. З погляду процесного підходу систему інформаційної безпеки підприємства можна представити як процес управління ризиками (рис.2.7), який включає в себе наступні складові.

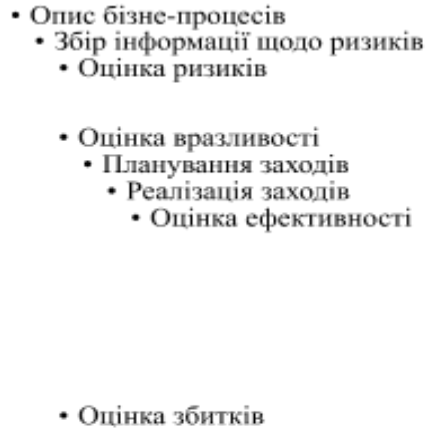


Рис. 2.7. Модель процесу управління ризиками для системи інформаційної безпеки в ТОВ «ІНКОМ-ІНВЕСТ»

1. Опис бізнес-процесів. Виконується коригування та аналіз бізнес-процесів. За критеріями, які визначаються в ході формування політики в галузі ризиків, здійснюється ідентифікація бізнес-процесів.

2. Збір ризиків. Проводиться для виявлення ступеня схильності підприємства загрозам, які можуть завдати істотної шкоди. Для цього

здійснюється аналіз його бізнес-процесів і опитування експертів предметної області. Результатом (виходом) даного процесу вважається класифікаційний перелік всіх потенційних ризиків.

До стандартних ризикам інформаційної безпеки ТОВ «ІНКОМ-ІНВЕСТ» відносяться:

- вилучення конфіденційної інформації з локальних місць;
- навмисне зміна інформації з метою знищення;
- копіювання важливих документів і передача конкуренту;
- незаконне проникнення в корпоративну мережу;
- знищення з технічних причин.

3. Оцінка ризиків. Визначаються характеристики ризиків і ресурси інформаційної системи. Основним результатом (виходом) даного процесу є перелік всіх потенційних ризиків з їх кількісними та якісними оцінками збитку і можливості реалізації, а додатковим - перелік ризиків, які не будуть відслідковуватися на підприємстві.

Процес оцінки ризиків на ТОВ «ІНКОМ-ІНВЕСТ» складається з наступних кроків:

- опис об'єкта і заходів захисту;
- ідентифікація ресурсу і визначення його кількісних показників;
- аналіз загроз інформаційної безпеки;
- оцінка вразливості;
- оцінка існуючих і передбачуваних засобів забезпечення інформаційної безпеки.

4. Планування заходів. Метою планування заходів щодо мінімізації ризиків є визначення термінів та переліку робіт по виключенню або мінімізації збитку у разі мінімізації ризику. Виділяються наступні види заходів з інформаційної безпеки:

- організаційні;
- правові;
- організаційно-технічні;
- програмні;
- інженерно-технічні.

5. Реалізація заходів. Під реалізацією заходів щодо мінімізації ризиків мається на увазі виконання запланованих робіт, контроль якості отриманих результатів та термінів. Результатом даного процесу є виконані роботи з мінімізації ризиків і час їх проведення.

6. Оцінка ефективності. Оцінка ефективності системи управління інформаційною безпекою - це системний процес отримання та оцінки об'єктивних даних про поточний стан системи, дії і події, що відбуваються в ній, встановлює рівень їх відповідності певним критеріям.

Оперативна реалізація заходів із розробки та охорони інформаційного складника економічної безпеки здійснюється послідовним виконанням певного комплексу робіт. Виділяють п’ять напрямів:

1) збирання різних видів необхідної інформації;

2) обробку та систематизацію одержаної інформації;

3) аналіз одержаної інформації;

4) захист інформаційного середовища підприємства, що охоплює: заходи для захисту суб'єкта господарювання від промислового шпіонажу з боку конкурентів або інших юридичних і фізичних осіб; технічний захист приміщень, транспорту, переговорів, різної документації від несанкціонованого доступу заінтересованих юридичних і фізичних осіб до закритої інформації; збирання інформації

про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій з метою припинення таких спроб;

5) зовнішню інформаційну діяльність.

Створення ефективної системи інформаційної безпеки є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією. Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарату. Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності.

Підприємство ТОВ «ІНКОМ-ІНВЕСТ» використовує основні правила інформаційної безпеки, до яких належать:

- розвідка;
- професіоналізм у встановленні контактів (мінімальні витрати часу і сил для пошуку інформації, необхідної для налагодження контакту);
- кваліфікація менеджера (витрати часу тільки на потрібних людей);
- уміння долати перешкоди, пошук варіантів і обхідних шляхів для дозволу виникаючих проблем;
- уміння завершувати операцію навіть з негативним результатом (усе ж краще, ніж відсутність якого-небудь результату).

Основними принципами інформаційної безпеки, яких дотримується ТОВ «ІНКОМ-ІНВЕСТ», є підтримання належного захисту інформації із забезпеченням її:

1. Цілісності - властивість захищеності, безпомилковості та повноти ресурсів система управління інформаційною безпекою (далі – СУІБ).

2. Конфіденційності - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.

3. Доступності - властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.

4. Спостережності - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів. Це в першу чергу стосується інформації з обмеженим доступом, до якої відносяться відомості що становлять комерційну таємницю, персональні дані та іншу конфіденційну інформацію.

Серед основних об'єктів на які розповсюджується дія інформаційної безпеки ТОВ «ІНКОМ-ІНВЕСТ» розглядаються наступні види ресурсів:

- інформаційні ресурси - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання співробітників, партнерів підприємства, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
- програмне забезпечення - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується на підприємства співробітниками та системами для

роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами тощо;

●фізичні ресурси - співробітники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо;

●сервісні ресурси - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх співробітники), послугами яких користується підприємство для отримання, використання, передачі та знищення ресурсів.

Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто ТОВ «ІНКОМ-ІНВЕСТ» використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Політика базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки. Підприємство ТОВ «ІНКОМ-ІНВЕСТ» використовуються наступні підходи щодо забезпечення інформаційної безпеки:

●створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;

●створено та затверджено перелік критичних бізнес-процесів;

●встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;

●забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;

●забезпечується парольний захист програмних та сервісних ресурсів;

●забезпечується антивірусний захист програмних та сервісних ресурсів;

●забезпечується захист мережі;

●забезпечується віддалений доступ до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);

●забезпечується ідентифікація та автентифікація всіх визначених ресурсів;

●забезпечується криптографічний захист інформації.

Всі співробітники підприємства ТОВ «ІНКОМ-ІНВЕСТ» обізнані та виконують вимоги інформаційної безпеки в роботі. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві ТОВ «ІНКОМ-ІНВЕСТ»:

- підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних;
- підсистема управління контролем доступу та ідентифікацією в інформаційній системі;

- підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів;
- підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних;
- підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування;
- підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації;
- підсистема захисту систем управління базами даних;
- підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства;
- підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму;
- підсистема захисту мобільних пристроїв;
- підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво ТОВ «ІНКОМ-ІНВЕСТ» повинно створювати співробітникам умови для систематичного навчання нормам та заходам інформаційної безпеки. На підприємстві складаються, діють, систематично тестуються та оновлюються плани безперебійного

функціонування діяльності підприємства на випадок різних непередбачуваних критичних ситуацій.

На шляху зміцнення інформаційної безпеки ТОВ «ІНКОМ-ІНВЕСТ» можна запропонувати такі кроки:

1) у рамках ресурсної безпеки

- вдосконалювання системи розрахунків; підвищення продуктивності праці;
- збільшення капіталовкладень у ресурсозбереження;
- стимулювання «ресурсного» напряму;

2) у рамках економічної безпеки

- застосування принципу дотримання критичних термінів кредитування; створення інформаційного центру, щоб постійно мати відомості про борги підприємства і перекрити канали витоку інформації: створення в структурі інформаційного центру спеціальної групи фінансових робітників, що перевіряла би податкові та інші обов'язкові платежі для виявлення можливої переплати і надавала зведення про маловикористовувані основні виробничі фонди з метою їхнього можливого продажу;
- використання нових форм партнерських зв'язків;

3) у рамках соціальної безпеки:

- наближення рівня оплати праці до показників розвитих країн, притягнення робітників до управлінських функцій;
- підвищення кваліфікації робітників;
- зацікавленість адміністрації підприємства у працевлаштуванні безробітних; розвиток соціальної інфраструктури підприємства;

- підвищення матеріальної відповідальності робітників за результати своєї праці.

Серед наявних засобів забезпечення безпеки підприємства, які в подальшому доцільно використовувати ТОВ «ІНКОМ-ІНВЕСТ» можна виокремити такі:

- технічні засоби (охоронно-пожежні системи, відео- та радіоапаратура, засоби виявлення вибухових приладів, бронежилети, огородження тощо);
- організаційні засоби (створення спеціалізованих формувань, що забезпечують безпеку підприємства);
- інформаційні засоби (друкована і відеопродукція з питань збереження конфіденційної інформації);
- фінансові засоби (без достатніх фінансових коштів неможливе функціонування системи економічної безпеки підприємства);
- правові засоби (підприємство повинне у своїй діяльності керуватися не лише виданими вищестоящими органами влади законами та підзаконними актами, але й розробляти власні локальні правові акти з питань забезпечення економічної безпеки підприємства);
- кадрові засоби (підприємство повинне бути забезпечене кадрами, що займаються питаннями економічної безпеки);
- інтелектуальні засоби (залучення до роботи кваліфікованих спеціалістів, наукових робітників, що дає змогу модернізувати систему безпеки підприємства).

Впровадження цих засобів одночасно не є можливим, адже повинно проходити в кілька етапів: виділення фінансових коштів; формування кадрових і організаційних засобів; розробка системи

правових засобів; залучення технічних, інформаційних та інтелектуальних засобів.

Отже, в умовах глобалізації забезпечення інформаційної безпеки на підприємстві ТОВ «ІНКОМ-ІНВЕСТ» повинно полягати постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, само тестування).

РОЗДІЛ 3. Напрями покращення рівня інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ»

3.1 Проблеми забезпечення інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ»

Якщо фірма досягає певних успіху у власному бізнесі, з'являється реальна загроза її інформаційної безпеки і безперервності бізнесу, пов'язаної з інтересом, що до неї проявляють конкуренти. Дані аспекти не тільки встановлюють значимість безпеки інформації, але і стають важливою складовою розвитку сучасної безпеки та безперервності бізнесу. Дане питання особливо актуальне в епоху інформаційного розвитку , що інтенсивними темпами змінює постіндустріальну епоху. Науково-технічний переворот відчуває весь світ, що змушує компанії відповідати на її виклики [24]. Абсолютно очевидно, що для ефективної протидії загрозам інформаційної безпеки та безперервності бізнесу потрібно, в першу чергу, усвідомити основу цього дійства, а потім - шукати шляхи вирішення проблеми.

Дані аспекти встановили актуальність та завдання дослідження, що складається з розкриття проблем надання інформаційної безпеки та безперервної діяльності бізнесу та пошуку ймовірних течій їх вирішення.

Як виявило дослідження даної проблеми, сучасний бізнес не може існувати і розвиватись на ринку без інформаційних технологій [39,40]. Загальноприйнятий факт, що приблизно 70% всесвітнього загального державного продукту певним чином залежить від даних, що

зберігаються в інформаційних системах. Ні в кого не викликає сумнівів той факт, що поступове впровадження технологій крім безумовної зручності призвело до серйозних проблем, однією з которих є проблема захисту інформації та забезпечення безпеки бізнесу.

Якщо говорити про вітчизняний бізнес в даному аспекті, що в Україні, нажаль, не проводяться дослідження, направлені на виявлення порушень інформаційної безпеки бізнесу. Пов'язане дане зі тим, що компанії, які отримали шкоду від хакерських атак, прагнуть не афішувати діні факти, а це не дозволяє виявити несанкціоновані проникення до їхньої інформаційної мережі.

Разом з тим з виникаючими в засобах масової інформації даних по цій проблемі йдеться, що має велику кількість слабких місць в захисті інформаційних атак [54-56]. Окрім того, хакерами часто бувають люди, які не маючи відповідної освіти в даній сфері.

Таким чином, слід зробити свій вибір з тим, яка безпосередня інформація може представляти зацікавленість конкурентів. Важливість рішення даної задачі заключається в тому, що від її рішення залежить ефективність сформованої системи безпеки і безперервності роботи бізнесу. У цьому аспекті слід здійснити SWOT-аналіз бізнесу, що дасть можливість виявити конкурентні переваги, що показують зацікавленість так само як для свого бізнесу, так і для конкурентів [32]. При цьому необхідно врахувати, що якості конкурентних переваг можуть бути технології, плани потоку фінансових та матеріальних потоків, стратегій розвитку, нові послуги чи продукти компанії, кадрові елементи, партнери компанії та інші.

Крім цього, необхідно враховувати, що ця діяльність буде мати значення тільки лише у випадку, коли в разі якщо інформація, яку

необхідно охороняти, передбачає справжню зацікавленість з боку суперників або конкурентів та дії відповідно до її охорони стануть економічно доцільні.

Також слід виявити, ту чи іншу інформацію, у якому розмірі, з якою періодичністю та у якому виді необхідно демонструвати інших негативних наслідків, з числа яких, найбільш серйозні - поява недовіри зі сторони контактної аудиторії (покупці , партнери, апарати урядового управління та регулювання, ділової сфери бізнесу, трейдери) .

Що стосується розкриття персон та установ, для яких, представляє зацікавленість інформації про бізнесі, в такому випадку тут необхідно виділити, що головну загрозу для бізнесу з точки зору надання його інформативної безпеки представляють безпосередньо суперники, які прагнуть отримати якомога більшу частку ринку [28,29]. Також необхідно виділити окрему увагу таким елементам безпеки та безперервної діяльності бізнесу, як можливість знищення та викривлення інформації, копіювання конфіденційних або секретних даних, закриття або обмеження доступу до інформації, необхідної компанії, несанкціонований доступ до неї.

Окремо необхідно враховувати ту обставина, що в фірмах невеликого та середнього бізнесу аж до цих часів проблеми захисту інформації та безперервної діяльності бізнесу вирішуються в рамках автоматизації діяльності [26].

Дослідження дозволило виявити 2 найважливіші проблеми на ТОВ «ІНКОМ-ІНВЕСТ», вирішення яких, проявляє прямий вплив на реалізацію планів компанії, націлених на надання інформаційної безпеки та безперервності роботи підприємства:

- вартість необхідних товарів та послуг;

- збереження бюджету на безпеку.

За минулі 3 роки ціна необхідних товарів та послуг збільшується в середньому на 10-20% в основному через результат збільшення витрат на програмне надання. Разом з тим має місце той факт, що продавці товарів-ІБ практикують еластичну цінову політику, коли ціна регулюється виходячи з бюджету і потреб конкретного замовника. Такий еластичний підхід дає можливість продавцям товарів-ІБ зберігати відповідний собі ступінь прибутковості та утримувати ринкову частину.

З іншою сторони, збільшення ціни товарів-ІБ змусить клієнтів поміняти власний підхід до підбору певних адміністративних рішень, націлених на надання інформаційної безпеки. Таким чином, будь-яка п’ята фірми зросли терміни здійсненні ІБ-планів, але крім того триває процедура підбору ІБ-товарів.

Необходімо виділити, то через декілька останніх років змінились критерії підбору товарів-ІБ в двох напрямках:

- компанії-клієнти почали більше приділяти уваги локалізації;
- предметом найбільш серйозного дослідження для компанії-клієнта стала ціна постанови. При цьому розмова проходить ніяк не про «прайсової вартості», а про загальну ціну володіння (TCO -Total Cost of Ownership) .

В умовах постійного зростання кількості відомих і появи нових видів інформаційних загроз перед великими підприємствами все частіше постає завдання забезпечення надійного захисту корпоративних мереж від шкідливих програм і мережевих атак.

Робота з інформацією в сучасних умовах відрізняється не тільки масивом і різноманіттям ресурсів, постійним оновленням технологій її

обробки, підвищеною увагою і контролем над персоналом, але і грамотним рівнем управління фірмою.

Відомо, що процес масового впровадження комп'ютерної техніки та інформаційних технологій поряд з прогресивним початком неминуче створює і додаткові проблеми. Вони пов'язані з реальними загрозами безпеці підприємств, з втратою стратегічно важливої інформації, а разом з цим і втратою керованості компанії.

З метою скорочення побічних явищ повсюдного використання нових інформаційних технологій керівництво організацій визначає стратегію своєї діяльності в інформаційній сфері. Стрижневим початком такої стратегії повинна бути інформаційна безпека, яка визначається як стан захищеності інтересів підприємств або організації в інформаційній сфері. Всі напрямки діяльності підприємства, в яких прямо або побічно використовуються інформаційні технології, фокусуються в рамках забезпечення інформаційної безпеки.

Як показує міжнародна практика, основна проблема в сфері забезпечення інформаційної безпеки полягає в створенні єдиного ефективного механізму, який дозволяв би своєчасно застосовувати на практиці нормативно-правові, законодавчі акти, які відповідають існуючим соціально-політичним і економічним умовам та досягнень в області інформаційних технологій. Розвиток технологій, сфери інформатизації робить актуальним питання забезпечення інформаційної безпеки.

Проблема забезпечення інформаційної безпеки має дві складові - технологічну й ідеологічну. Перша - пов'язана з розробкою і впровадженням інформаційних ресурсів, системи захисту

інформаційних баз, друга - з поширенням інформації, її впливом на життя особистості, суспільства, держави [3; С.238].

Практично будь-яка нова технологія тягне за собою соціально-економічні зміни в суспільстві, впливає на міжнародні відносини. На сьогоднішній день можна говорити про створення загальносвітового інформаційного простору. Інформація, інформаційні технології характеризуються такими властивостями як транскордонність, проникність, мають можливість повсюдного використання, стають доступними незалежно від національних кордонів.

Під погрозами інформації прийнято розуміти потенційні чи реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння охоронюваними відомостями.

Такими діями є:

- ознайомлення з інформацією різними шляхами і способами без порушення її цілісності;
- модифікація інформації в кримінальних цілях як часткове або значна зміна складу і змісту відомостей;
- руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

В кінцевому підсумку протиправні дії з інформацією призводять до порушення її конфіденційності, повноти, достовірності і доступності, що в свою чергу призводить до порушення, як режиму управління, так і його якості в умовах помилкової або неповної інформації. Кожна загроза тягне за собою певний збиток - моральної чи матеріальної, а захист і протидія загрозі покликане знизити його величину, в ідеалі - повністю,

реально - значно або хоча б частково. Але і це вдається далеко не завжди.

Управління підприємством не може ефективно проводитися без достатньої оперативної, надією, своєчасної та достовірної інформації. Інформація є основою управлінського процесу, і від того, наскільки вона досконала, багато в чому залежить якість управління підприємством. Інформаційна діяльність менеджера вимагає від нього чіткої організації процесу збору, аналізу і обробки інформації, причому він повинен вміти визначати важливість або другорядність, що надходить. Досвідчений менеджер також повинен мати впорядковувати комунікації і обмін інформацією в рамках підприємства і фірми.

Керуюча система отримує від керованої системи інформацію про стан заданих нею техніко-економічних параметрів в процесі виробничої і фінансово-господарської діяльності. На основі отриманої інформації керуюча система (менеджмент) виробляє команди управління і передає їх в керовану систему для виконання. Інформація, яка функціонує на підприємстві в процесі управління, може бути класифікована наступним чином:

- за формою відображення (візуальна, аудіовізуальна та змішана);
- за формою подання (цифрова, літерна, кодованих);
- за роллю в процесі управління (аналітична, прогнозна, звітна, наукова, нормативна)
- за якістю (достовірна, вероятностно достовірна, недостовірна, неправдива);

- по можливості використання (необхідна, достатня, надлишкова);
- за ступенем оновлюється (постійна, змінна);
- за ступенем діяльності підприємства (економічна, управлінська, соціальна, технологічна);
- за джерелом виникнення (внутриорганизационная, зовнішня);
- за ступенем перетворення (первинна, похідна, узагальнена);
- по виду носія (друкований текст, мікрофільм, кінофільм, відеофільм, машинний носій);
- за часом надходження (періодична, постійна, епізодична, випадкова) [9; С.7].

Як приклад наведемо три основних напрямки збору інформації про конкурента.

Інформація про ринок:

-
- ціни, знижки, умови договорів, специфікація продукту;
- обсяг, історія, тенденція і прогноз для конкретного продукту;
- частка на ринку і тенденції її зміни;
- ринкова політика і плани;
- відносини з споживачами і репутація;
- чисельність і розміщення торгових агентів;
- канали, політика і методи збуту;
- програма реклами.
- Інформація про виробництво і продукції:
- оцінка якості та ефективності;
- номенклатура виробів;

- технологія і устаткування;
- рівень витрат;
- виробничі потужності;
- розміщення і розмір виробничих підрозділів і складів;
- спосіб упаковки;
- доставка;
- можливості проведення науково-дослідних робіт (НДР).

Інформація про організаційні особливості і фінансах:

- визначення осіб, які беруть ключові рішення;
- філософія осіб, які беруть ключові рішення;
- фінансові умови і перспективи;
- програми розширення і придбань;
- головні проблеми та можливості;

Велика увага з боку менеджера повинна приділятися питанням збереження інформації та запобігання її витоку [43; С.180].

Цікавим видається вислів англійських фахівців в області захисту інформації: "Немає сенсу ретельно перевіряти приміщення перед засіданням, якщо кава в приміщення подається неперевіреними співробітником без відповідного спостереження"

Залежно від форми подання інформація може бути розділена:

- Мовна інформація. Виникає в ході ведення в приміщеннях розмов, роботи систем зв'язку, звукопідсилення і звуковідтворення.
- Телекомунікаційна інформація. Циркулює в технічних засобах обробки і зберігання інформації, а також в каналах зв'язку при її передачі.

- Документована інформація (документи). Відносять інформацію, представлену на матеріальних носіях разом з ідентифікують її реквізитами.

3.2 Шляхи вдосконалення рівня інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ»

Слід мати на увазі, те що численні заходи безпеки вимагають досить великих обчислювальних ресурсів, що в свою чергу значно впливає на процес оброблення інформації. Тому сучасний аспект до вирішення цієї проблеми полягає у використанні в АСУ основ ситуаційного управління безпекою інформаційних ресурсів. Сутність подібного підходу полягає в тому, що необхідний рівень захищеності інформації встановлюється в узгодженні з обстановкою, що характеризує відповідність між цінністю опрацьованої інформації, витратами (зменшенням продуктивності АСУ, допоміжними витратами оперативної пам'яті та інше), які потрібні з метою досягнення цього рівня, та ймовірними підсумковими витратами.

Необхідні характеристики безпеки інформаційних ресурсів формуються на протязі ситуаційного планування при підготовці науково-технічного процесу оброблення інформації з урахуванням сформованої ситуації, але крім того в період процесу обробки. Підбираючи запобіжні заходи, потрібно брати до уваги не тільки безпосередні витрати на закупівлю оснащення та проектів, проте також витрати на введення нововведення, на підготовка та перепідготовку персоналу. Значущим обставиною вважається порівнянність новітнього ресурсу з сформованою апаратно-програмної текстурою предмета.

Іноземний навик у сфері безпеки інтелектуальної майна та вітчизняний досвід з захисту державних таємниць демонструють, що результативним здатний бути тільки складний вид безпеки, який

поєднує в собі подібні тенденції безпеки,як правове, організаційне та інженерно-технічне.

Правова спрямованість враховує розвиток сукупності законодавчих актів, нормативно-правових документів, тверджень, посібників, керівництв, умови яких, вважаються невід'ємними у рамках сфери їх діяльності в системі безпеки інформації.

Організаційне направлення - це регулювання виробничої діяльності та відносин виконувачів на нормативно-законній основі таким способом, що оприлюднення, витік та несанкціонований допуск до конфіденційної інформації робляться неможливими або значно ускладнюються через результат виконання координаційних робіт.

До координаційним подій належать:

- заходи, що виконуються при проектуванні, будівництві та оснащенні посадових та виробничих будівель;
- заходи, що виконуються при виборі персоналу;
- організація та підтримання достовірного пропускного порядку, захисту приміщень та територій, контроль відвідувачів;
- організація зберігання та застосування документів та носіїв конфіденційної інформації;
- організація безпеки даних;
- організація регулярного навчання співробітників.

Один з ключових частин координаційного надання інформаційної захищеності фірми вважається Відділ інформативною захищеності (ВІЗ - апарат управління концепцією охорони та безпеки даних). Безпосередньо від висококласної підготовленості працівників служби інформаційної безпеки, присутності у них в арсеналі сучасних методів управління безпекою.

Головне завдання функціонування ВІЗ, застосовуючи організаційні заходи та програмно-апаратні ресурси, - виключити або хоча б звести до мінімуму ймовірність порушення політики безпеки, в останньому випадку, своєчасно зазначити також ліквідувати результати порушень.

З метою надання ефективної діяльність ВІЗ слід встановити її повноваження та прямі обов'язки, але крім того принципи взаємодії з іншими підрозділами згідно проблемам захисту даних в предметі. Чисельність служби зобов'язана бути достатньою з метою виконання абсолютно всіх покладених на них функцій. Переважно, для того щоб штатна структура служби не мав зобов'язань, пов'язаних з функціонуванням предмету захисту. Відділ інформативної захищеності зобов'язаний бути забезпечиним абсолютно всіма критеріями, важливими для виконання власних функцій.

Ядром інженерно-технологічного тенденції вважаються програмно-апаратні ресурси безпеки інформації, до яких належать машинні, електромеханічні, електронні, оптичні, лазерний, радіотехнічні, радіолокаційні також інші прилади, концепції та споруди, призначені для надання захищеності та безпеки даних.

Політика безпеки встановлює образ концепції безпеки інформації у сукупності правових норм, організаційних (законних) заходів, комплексу програмно-технічних засобів та процедурних висновків, націлених в опір загрозам для вилучення або мінімізації можливих наслідків прояву інформативних впливів. Вже після прийняття цього або іншого варіанту політики захищеності слід дати оцінку ступеня безпеки інформативною концепції. Безумовно, оцінка безпеки виконується відповідно до сукупності показників, головними з яких, вважаються ціна, результативність, можливість втілення.

Якщо заплановані заходи встановлені, слід проконтролювати їх ефективність, і те що остаточні ризики стали прийнятними. Тільки лише після цього можна планувати дату найближчої переоцінки. У іншому випадку буде потрібно вивчити допущені похибки та здійснити повторну процедура розгляду уразливості зі урахуванням змін в концепції безпеки.

Один з можливих способів атестації безпеки системи - запрошення хакерів для злому без попереднього повідомлення персоналу мережі. Для цього виділяється група з двох-трьох чоловік, що мають високу професійну підготовку. Хакерам надається в розпорядження автоматизована система в захищеному виконанні, і група протягом 1-3 місяців намагається знайти вразливі місця і розробити на їх основі тестові кейси для обходу механізмів захисту. Наймані хакери представляють конфіденційну доповідь за результатами роботи з оцінкою рівня доступності інформації і рекомендацій щодо поліпшення захисту.

На етапі створення плану захисту відповідно до обраної політики безпеки розробляється план його реалізації. План захисту є документом, що вводить в дію системи захисту інформації, який затверджується керівником організації. Планування пов'язано не тільки з найкращим використанням всіх можливостей, якими володіє компанія, в тому числі виділених ресурсів, а й із запобіганням помилкових дій, що можуть призвести до зниження ефективності вжитих заходів щодо захисту інформації.

План захисту інформації на об'єкті повинен включати:

- опис захищення системи (основні характеристики об'єкта, що захищаються: призначення об'єкта, перелік вирішуваних завдань, конфігурація, характеристики і розміщення технічних засобів і програмного забезпечення, перелік категорій інформації (пакетів, файлів, наборів і баз даних, в яких вони містяться), які підлягають захисту, і вимог щодо забезпечення доступу, конфіденційності, цілісності цих категорій інформації, список користувачів і їх повноважень по доступу до ресурсів системи і т. п.);
- мета захисту системи та шляхи забезпечення безпеки автоматизованої системи і циркулюючої в ній інформації;
- перелік значущих загроз безпеки автоматизованої системи, від яких вимагається захист, і найбільш ймовірних шляхів нанесення шкоди;
- політику інформаційної безпеки;
- план розміщення коштів і функціональну схему системи захисту інформації на об'єкті;
- специфікацію засобів захисту інформації та кошторис витрат на їх впровадження;
- календарний план проведення організаційних і технічних заходів щодо захисту інформації, порядок введення в дію засобів захисту;
- основні правила, що регламентують діяльність персоналу з питань забезпечення інформаційної безпеки об'єкта (особливі обов'язки посадових осіб, які обслуговують автоматизовану систему);
- порядок перегляду плану і модернізації засобів захисту.

Перегляд плану захисту здійснюється при зміні таких компонентів об'єкта:

- кадрів;
- архітектури інформаційної системи (підключення інших локальних мереж, зміна або модифікація використовуваних засобів обчислювальної техніки або ПО);
- територіального розташування компонентів автоматизованої системи.

В рамках плану захисту необхідно мати план дій персоналу в критичних ситуаціях, тобто план забезпечення безперервної роботи та відновлення інформації. Він відображає:

- мету забезпечення безперервності процесу функціонування автоматизованої системи, відновлення її працездатності та шляхи її досягнення;
- перелік і класифікацію можливих кризових ситуацій;
- вимоги, заходи та засоби забезпечення безперервної роботи та відновлення процесу обробки інформації (порядок створення, зберігання і використання резервних копій інформації, ведення поточних, довгострокових і аварійних архівів; склад резервного обладнання та порядок його використання);
- обов'язки та порядок дій різних категорій персоналу системи в кризових ситуаціях, при ліквідації їх наслідків, мінімізації завдається шкоди і при відновленні нормального функціонування системи.

Якщо підприємство реалізовує взаємообмін електронними паперами з партнерами відповідно до здійсненню спільних замовлень, в

такому випадку слід у проєкт безпеки ввести угоду про режими обміну електронними паперами, у якому відображаються відповідні питання:

- розподіл відповідальності суб'єктів, що беруть участь у процесах обміну електронними паперами;
- встановлення режиму підготовки, дизайну, передачі, прийому, контролю оригінальності та цілісності електронних паперів;
- режиму генерації, сертифікації та поширення головної інформації (ключів, паролів);
- режим дозволу диспутів у разі появи інцидентів.

Проект захисту інформації передбачає собою комплекс текстуально-графічних документів, з цієї причини нарівні із елементами даного пакета у нього можуть вступати:

- положення про комерційну таємницю, що характеризує список даних, елементів комерційної таємниці, також процедура його встановлення, але крім того прямі обов'язки посадових осіб відповідно до безпеки комерційної таємниці;
- положення про охорону даних, що регламентує всі без винятку тенденції роботи згідно здійсненні політичні діячі захищеності, але крім того кілька додаткових посібників, законів, тверджень, визначених специфікою предмета охорони.

Реалізація плану захисту (управління концепцією захисту) має на увазі дослідження необхідних паперів, завершення угод з постачальниками, установка, налаштування оснащення також.

Управління - процедура спрямованого впливу на об’єкт, що виконується для компанії його функціонування відповідно до встановленого планом.

Керівництво інформативною захищеністю повинно бути:

- стабільним до чинним втручанням порушника;
- постійним, що забезпечує безперервне вплив в процедура охорони;
- таємним, неможливо що дозволяє виявляти систему управління охороною даних;
- експлуатаційним, що забезпечує ймовірність вчасно також адекватно реагувати на дії лиходіїв також здійснювати адміністративні постанови до встановленого терміну.

Крім цього, постанови згідно захисту даних зобов'язані бути аргументованими з точки зору багатостороннього урахування обставин виконання встановленої проблеми, використання різних модифікацій, обчислених також інформативних питань, експертних концепцій, навички та різних інших відомостей, що збільшують достовірність вихідної інформації та прийнятих висновків.

Ознакою продуктивності управління безпекою інформації вважається період циклу управління при встановленому списку прийнятих висновків. В оборот управління вступає отримання необхідної інформації для оцінки умови, твердження постанови, розвиток певних установок також їх виконання. У властивості аспекту продуктивності здатний застосовуватися період взаємодії концепції безпеки інформації на недотримання, що не повинно бути перевищувати період застарівання інформації відштовхуючись від її значення.

Так само як демонструє створення справжніх АСУ, єдиний з методів (граней, засобів та подій) надання захищеності інформації не вважається абсолютно надійним, але найбільший результат досягається

присутністю злиття всіх їх у цілу систему безпеки інформації. Тільки найкраща сукупність координаційних, промислових та програмних подій, а так само як і постійний інтерес та нагляд потребує підтримання концепції безпеки в чинному перебуванні, що дадуть можливість з максимальною віддачею гарантувати дозвіл постійної задачі.

Методологічні основи забезпечення інформаційної безпеки є досить загальними рекомендаціями, що базуються на світовому досвіді створення подібних систем. Завдання кожного фахівця із захисту інформації - адаптувати абстрактні положення до своєї конкретної предметної області (організації, банку), в якій завжди знайдуться свої особливості і тонкощі.

Аналіз вітчизняного та зарубіжного досвіду переконливо доводить необхідність створення цілісної системи інформаційної безпеки компанії, що погоджує оперативні, оперативно-технічні та організаційні заходи захисту. Причому система безпеки повинна бути оптимальною з точки зору співвідношення витрат і цінності захищених ресурсів. Необхідна гнучкість і адаптація системи до швидко-мінливих чинників навколишнього середовища, організаційної та соціальної обстановці в організації. Досягти такого рівня безпеки неможливо без проведення аналізу існуючих загроз і можливих каналів витоку інформації, а також без вироблення політики інформаційної безпеки на підприємстві. У підсумку повинен бути створений план захисту, який реалізує принципи, закладені в політиці безпеки.

Але існують і інші складності і «підводні камені», на які обов'язково потрібно звернути увагу. Це проблеми, виявлені на практиці і слабо піддаються формалізації: проблеми не технічного або

технологічного характеру, які так чи інакше вирішуються, а проблеми соціального і політичного характеру.

Відсутність розуміння у персоналу і керівників середньої та нижньої ланки необхідності проведення робіт з підвищення рівня інформаційної безпеки - на цій сходинці управлінських сходів, як правило, не видно стратегічних завдань, що стоять перед організацією. Питання безпеки при цьому можуть викликати навіть роздратування - вони створюють «непотрібні» труднощі.

Часто наводяться наступні аргументи проти проведення робіт та вжиття заходів щодо забезпечення інформаційної безпеки:

- поява додаткових обмежень для кінцевих користувачів і фахівців підрозділів, що обтяжує їх користування автоматизованою системою організації;
- необхідність додаткових матеріальних витрат як на проведення таких робіт, так і на розширення штату фахівців, що займаються проблемою інформаційної безпеки.

Зазначена проблема є однією з основних. Всі інші питання так чи інакше виступають в якості її наслідків. Для її подолання важливо вирішити такі завдання: по-перше, підвищити кваліфікацію персоналу в області захисту інформації шляхом проведення спеціальних зборів, семінарів; по-друге, підвищити рівень інформаційної обізнаності персоналу, зокрема, про стратегічні завдання, що стоять перед організацією.

Протистояння служби автоматизації і служби безпеки організацій - ця проблема обумовлена родом діяльності і сферою впливу, а також

відповідальності цих структур всередині підприємства. Реалізація системи захисту знаходиться в руках технічних фахівців, а відповідальність за її захищеність лежить на службі безпеки. Фахівці служби безпеки хочуть будь-що-будь обмежити за допомогою міжмережевих екранів весь трафік. Але люди, що працюють у відділах автоматизації, не бажають вирішувати додаткові проблеми, пов'язані з обслуговуванням спеціальних засобів. Такі розбіжності не кращим чином позначаються на рівні захищеності всієї організації.

Вирішується ця проблема, як і більшість подібних, чисто управлінськими методами. Важливо, по-перше, мати в організаційній структурі фірми механізм вирішення подібних конфліктів. Наприклад, обидві служби можуть мати єдине начальство, яке буде вирішувати проблеми їх взаємодії. По-друге, технологічна і організаційна документації повинні чітко і грамотно ділити сфери впливу і відповідальності підрозділів.

Взаємовідносини між керівниками можуть бути різними. Іноді при проведенні робіт з дослідження інформаційної захищеності та чи інша посадова особа проявляє зацікавленість в результатах цих робіт. Дійсно, дослідження - це досить сильний інструмент для вирішення їх приватних проблем і задоволення амбіцій. Висновки і рекомендації, записані в звіті, використовуються як план до подальших дій того чи іншого ланки. Така ситуація є вкрай небажаним чинником, так як спотворює сенс проведення робіт і вимагає своєчасного виявлення та ліквідації на рівні вищого керівництва підприємства. Найкращим варіантом є ділові взаємини, коли на перше місце ставляться інтереси організації, а не особисті.

Низький ступінь виконання запланованої програми операцій згідно формуванню системи безпеки даних - це досить звичайна обстановка, коли стратегічні цілі і задачі губляться на рівні виконання. Головний керівник бере на себе рішення про необхідність поліпшення систем інформативною захищеності. Підряджається самостійна консультаційна компанія, яка виконує перевірка наявної концепції охорони даних. По закінченню створюється доповідь, що містить всі без винятку необхідні поради згідно безпеки інформації, доопрацювання наявного документообігу у сфері інформативної захищеності, згідно введенню технічних засобів інформації та організаційних граней, подальшої допомоги утвореної системи. Проект захисту містить короткочасні та довготривалі події. Потім поради переходять в виконання у один з підрозділів. Також тут важливо, для того щоб вони не потонути у болоті бюрократії, нерозторопність персоналу та в багатьох інших факторах. Виконавець здатний бути слабо поінформований, мало досяг успіху або просто ніяк не зацікавлений у виконанні праць. Важливо, щоб генеральний директор перевірив здійснення запланованого проекту, щоб не втратити.

Низька кваліфікація експертів згідно охорони даних - цей підхід може не розглядатися значною перешкодою. Проблема в тому, що під план захисту, так само як принцип, вводиться подібна подія, так само як збільшення кваліфікаційних експертів у сфері інформаційної безпеки в компанії. Для експертів інших галузей можуть проводитися семінари відповідно до основ компанії безпеки інформації. Необхідно правильно оцінювати справжню кваліфікацію працівників, зайнятих здійсненням проекту захисту. Нерідко помилкові висновки або нездатність

використовувати засоби безпеки в практиці призводять до складнощів при здійсненні рекомендованих дій.

ВИСНОВКИ

В результаті проведеного дослідження напрямів покращення рівня інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ» можна зробити наступні висновки.

У ході роботи було досліджено сутність поняття інформаційної безпеки, досліджені принципи використання систем інформаційної безпеки в системі управління підприємством, охарактеризовано основні методи використання та визначення місця інформаційної безпеки на підприємстві.

В результаті проведеного дослідження виявлено цілі та шляхи використання інформаційної безпеки в вітчизняних організацій.

Інформативна безпека компанії досягається єдиним комплексом координаційних та промислових заходів, націлених на захист колективних відомостей. Координаційні заходи містять документовані процедури та принципи діяльність з різними типами даних, IT-сервісами, засобами безпеки також . Промислові заходи складаються у застосуванні апаратних та програмних засобів контролю допуску, прогнозу витоків, антивірусної безпеки, міжмережевого екранування.

Проблеми концепцій інформативною захищеності компанії різноманітні. Дане надання захищеного збереження даних в різних носіях; охорона відомостей, переданих каналами взаємозв'язку; розподіл допуску до різних типів документації; створення резервних копій, після-аварійне відновлення інформаційних .

Визначено, що протягом 2016-2018 рр. відбувалося зростання чистого доходу підприємства, що призвело до зростання чистого

прибутку підприємства. Сумарні доходи підприємства мали аналогічну динаміку до зростання на 31,24% за результатом 2017 року та на 22,95% за результатом 2018 року і становили 5879,4 тис. грн. та 7228,5 тис. грн. відповідно. Рентабельність власного капіталу 2016 році становив 28,83%, а в 2017 році, зменшившись на 13,456%, становив 15,378%. В 2018 році даний показник знову зріс – на +1,648%, і становив, таким чином, 17,025%. Рентабельність послуг підприємства в 2017 році становила 24,84% (сам показник зменшився на 18,79%), а в 2018 році показник зріс до рівня 25,85%(+1,016%). Динаміка даного показника свідчить про зростання ефективності та вигідності послуг, що здійснює підприємство. Динаміка коефіцієнту покриття в 2018 році свідчить про те, що підприємство збільшує обсяг оборотних коштів та зменшує борги, отже, може ліквідувати свої борги.

Досліджено, що основними цілями інформаційної безпеки на підприємстві ТОВ «ІНКОМ-ІНВЕСТ» є: конфіденційність інформації, тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб; неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб; цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), яка полягає в її існуванні в неспотвореному вигляді (незміненому по відношенню до деякому фіксованому її станом); доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до інформації, що їх цікавить; мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів; облік усіх процесів, пов'язаних з ризиками.

Система управління інформаційною безпекою на ТОВ «ІНКОМ-ІНВЕСТ» є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Встановлено, що в умовах глобалізації забезпечення інформаційної безпеки на підприємстві ТОВ «ІНКОМ-ІНВЕСТ» повинно полягати постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, само тестування).

РЕЗЮМЕ

Кваліфікаційна робота на тему «Інформаційна безпека бізнесу сучасної організації» виконана на базі практики ТОВ «ІНКОМ-ІНВЕСТ».

Метою кваліфікаційної роботи магістра є розробка шляхів вдосконалення інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ» теоретичних основ та сутності методів вдосконалення систем інформаційної безпеки, систематизація, закріплення та поглиблення знань набутих у процесі навчання та їх практичної реалізації, що полягають у розробці рекомендацій щодо вдосконалення систем інформаційної безпеки на ТОВ «ІНКОМ-ІНВЕСТ».

У першому розділі кваліфікаційної роботи було визначено сутність поняття інформаційної безпеки, досліджені принципи використання концепцій та правил інформаційної безпеки в системі управління підприємством, охарактеризовано основні методи обґрунтування та визначення місця використання систем інформаційної безпеки.

У другому розділі було надано загальну характеристику ТОВ «ІНКОМ-ІНВЕСТ», визначено особливості організаційної структури ТОВ «ІНКОМ-ІНВЕСТ» та проаналізовано економічні показники діяльності чинного підприємства.

У третьому розділі надані рекомендацій щодо вдосконалення систем інформаційної безпеки на актуальність теми дослідження.

Одержані результати, що мають прикладний характер, використані на практиці підприємства ТОВ «ІНКОМ-ІНВЕСТ».

Рік виконання дипломної роботи - 2019.

Рік захисту роботи - 2019.

RESUME

Qualification work on the topic "Information security of business of modern organization" was performed on the basis of the practice of LLC "INKOM-INVEST".

The purpose of the master's qualification work is to develop ways to improve information security at INCOM-INVEST LLC theoretical bases and essence of methods for improving information security systems, systematize, consolidate and deepen the knowledge acquired in the course of training and their practical implementation, which are to develop recommendations information security at INCOM-INVEST LLC.

In the first section of the qualification work the essence of the concept of information security was defined, the principles of using the concepts and rules of information security in the enterprise management system were investigated, the basic methods of substantiation and determination of the place of use of information security systems were characterized.

In the second section, the general characteristics of INKOM-INVEST LLC were presented, the features of the organizational structure of INKOM-INVEST LLC were determined, and the economic indicators of the activity of the current enterprise were analyzed.

The third section provides recommendations for improving information security systems for the relevance of the research topic.

The obtained results, which are applied in nature, were used in the practice of the company LLC INKOM-INVEST.

Year of completion of the thesis - 2019.

Year of protection of work - 2019.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакумов В.М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони / В.М. Абакумов // Форум права. – 2012. – № 4. – С. 10-16. – [Електронний ресурс]. – Режим доступу: http://arhive.nbuv.gov.ua/e-journals/FP/2012-4/12avmapo.pdf
2. Асоціації користувачів електронно-обчислювальних машина США - [Електронний ресурс]. – Режим доступу: https://ethics.acm.org
3. Басовский Л.Е., Протасьев В.Б. Управление качеством. М. : ИнфраМ., 2002.
4. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – С. 343–384.].
5. Белошапка В.А. Управленческая результативность: системный подход на работу и развитие менеджеров: учеб. [для практикующих менеджеров] / В.А. Белошапка, И. В. Нудьга. К.: Агентство "Стандарт", 2007. 270 с.
6. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005. -432 с.
7. Бондарь И. Проблемы информационной безопасности в условиях переходного общества // Персонал. - 2003. - № 8. - С. 47-48.
8. Борсуковский Ю. Подходы и решения : Информационная безопасность // Мир денег. - 2001. - № 5. - С. 41-42
9. Бєляков, К. І. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні / К.І.

Бєляков, Ю.П. Мірошник // Стратегічна панорама. – 2004. – № 3. – С. 171-177

10. Верескун М.В. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М.В. Верескун // Економіка і організація управління. – 2014. – № 1 (17). – С. 54-60.
11. Власова Л.А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.
12. Воськало Н.М. Внутрішній контроль власного капіталу підприємства в системі управління його діяльності / Н.М. Воськало // Збірник науково-технічних праць, Науковий вісник НЛТУ України. 2012. Вип. 22.9. С. 174-179
13. Господарський кодекс України: Кодекс України від 16.01.2003 № 436- IV / Верховна Рада України. – К.: Юрінком Інтер, 2006. 304 с.
14. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть // Вісник Київського університету імені Т.Шевченка. - 1999. - Вип. 14: Міжнародні відносини. - С. 46-48
15. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. - 2003. - № 5. - С. 2-3
16. Дафт Р.Л. Менеджмент [Текст] / Р.Л. Дафт; Пер. с англ. СПб.: Питер, 2007. 6-е изд.864 с.
17. Друкер П. Задачи менеджмента в XXI веке: Учебное пособие /Друкер Питер; Пер.с англ. и редакция Н.М.Макаровой. Москва. Санкт-Петербург. Киев : Вильямс, издательский дом, 2001. 272с.
18. Ермолович Л.Л. Анализ хозяйственной деятельности предприятия: учеб. пособие / Л.Л. Ермолович, Л.Г. Сивчик, Г.В. Толкач; Под общ. ред. Л.Л. Ермолович. Мн.: Интерпрессервис; Экоперспектива, 2007. 576 с.

19. Єдинак Т.С. Проблеми управління дебіторською заборгованістю підприємств в умовах фінансово – економічної кризи / Т.С. Єдинак // Держава та регіони. 2010. № 3. С. 54 – 57.
20. Закон України «Про охорону прав на комерційну таємницю» - [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1404-2008-%D1%80
21. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: від 09.01.2007 р., № 537.
22. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова. – [Електронний ресурс]. – Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3893
23. Захаров Е. Информационная безопасность или опасность отставания?// Права людини. - 2000. - № 1 . - С. 3-5
24. Журавель М.Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства / М.Ю. Журавель, Т.В. Полозова, О.В. Стороженко // Вісник економіки транспорту і промисловості. – 2011. – № 33. – С. 171-177.
25. Інформаційна безпека України: проблеми та шляхи їх вирішення // Національна безпека і оборона. - 2001. - № 1. - С. 60-69
26. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами // Альманах економічної безпеки. - 1999. - № 2. - С. 15-17
27. Карпюк О.А. Прибуток як економічна категорія в Х-економіці / О.А. Карпюк // Вісник ЖДТУ. 2008. №1 (39). С.32-38.

28. Кірсанова Т.О. Система управління власним капіталом підприємства [Текст] / Т.О. Кірсанова, Н.О. Коляда // Вісник Сумського державного університету. Серія Економіка. 2010. № 1, Т. 2. С. 58-63.
29. Конституція України: Закон Верховної Ради України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. №30. Ст. 141.
30. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. -К.: Кондор, 2005. -382 с.
31. Костенко Т.Д., Підгора Е.О. Економічний аналіз і діагностика стану сучасного підприємства: навч. посібник / За ред. Костенко Т.Д. та ін. – К.: ЦНЛ, 2005. – 400 с.
32. Кучеренко Т. Є. Теоретичне обґрунтування фінансових результатів в контексті моделі балансу / Т. С. Кучеренко // Вісник ХНАУ. Серія "Економіка АПК і природокористування". – 2009. – № 13. – С. 230-237.
33. Легомінова С.В. Теоретичні засади інформаційної безпеки підприємства / С.В. Легомінова // Економіка. Менеджмент. Бізнес. – 2015. – № 3 (13). – С. 87-92.
34. Литвиненко О. Інформація і безпека // Нова політика. - 1998. - № 1. - С. 47-49.
35. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування Інформаційні системи в менеджменті//А.А. Литвинюк. – [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

36. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский,; Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій . -Одеса, 2001. -164 с.
37. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України / А.І. Марущак. – 2011. – № 21. – С. 92-95.
38. Марюта О.М. Адаптивне управління прибутком підприємства / О.М. Марюта, О.К. Єлисеєва // Фінанси України. 2004. №3. С. 175-182.
39. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев. – Електронний ресурс. – Режим доступу:http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-isootvetstviya-5386161
40. Мацків О.І. Аналіз перспективних стандартів забезпечення інформаційної безпеки / О.І. Мацків, К.Б. Айвазова // Проблеми технічного регулювання та якості: IV Всеукр. наук.-практ. конф. (9-10 жовтня 2014 р.). – Одеса: ОДАТРЯ, 2014. – С. 39-42.
41. Мельник О. В. Особливості формування власного капіталу підприємства / О. В. Мельник, Л. І. Данілова, Т. Г. Венгуренко, А. А.Степаненко // Науковий вісник Національного університету ДПС України (економіка, право), 2010. 1(48). С. 94- 98.
42. Менеджмент організацій: Підручник. Колектив авторів за заг. ред. Л.І.Федулової. К.: Либідь, 2004. 448 с.
43. Мескон М.Х.,Альберт М., Хедоури Ф. Основы менеджмента: Пер.с англ. – М.: Дело, 2002. – 702с.

44. Мних Є.В. Аналіз і контроль в системі управління капіталом підприємства : монографія / Є.В. Мних, А.Д. Бутко, О.Д. Большакова, Г.О. Кравченко, Г.І. Никонович / за ред. проф. Є.В. Мниха. К. : Вид-во КНТЕУ, 2005. 232 с.
45. Моляков Д.С. Самофинансирование / Д.С. Моляков, С.В. Большаков. М.: Финансы и статистика, 2009. 159 с.
46. Момот Т.В. Сучасні моделі управління дебіторською заборгованістю підприємства / Т.В. Момот, Г.М. Бреславська // Науково – технічний збірник "Комунальне господарство міст". 2009. №85. С. 201 – 211.
47. Найт Ф. Риск, неопределенность и прибыль / Ф.Найт ; пер. с англ. М.Я. Каждана; Центр эволюц.экономики. – М.: Дело, 2003. – 359 с
48. Орлов О.О. Планування діяльності промислового підприємства. підручник / О.О. Орлов. – К.: Скарби, 2002. – 336 с.
49. Осовська Г.В. Менеджмент організацій: навч. посібник / Г.В. Осовська, О.А. Осовський. К.: Кондор, 2009. 680 с.
50. Пилипенко О. Формула безопасности : Информационная безопасность// СНІР. - 2005. - № 12. - С. 72-73
51. Правове забезпечення інформаційної діяльності в Україні/ Володимир Горобцов, Андрій Колодюк, Борис Кормич та ін.; Ред. І. С. Чиж; Ін-т держави і права ім. В.М.Корецького, Нац. Академія Наук України, Держ. комітет телебачення і радіомовлення України. -К.: Юридична думка , 2006. -384 с.
52. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. - 2001. - № 1. - С. 16-28
53. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев. – Електронний ресурс. – Режим доступу:

http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161

54. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Текст] / О.А. Сороківська, В.Л. Гевко // Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки. – 2016. – № 2. – Т. 2. – С. 32-35.
55. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 08.00.04 / М.Ю. Танцюра. – Сімферополь, 2012. – 21 с.
56. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) / В. Цимбалюк // Підприємництво, господарство і право. – 2011. – № 3. – С. 88-91.
57. Чередниченко А.О. Організаційно-економічне забезпечення управління інформаційною безпекою підприємств будівельної галузі: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 21.04.02 «Економічна безпека суб'єктів господарської діяльності» / А.О. Чередниченко. – Харків, 2016. – 21 с.
58. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ // Актуальні проблеми економіки. - 2006. - № 10. - С. 220 - 225.
59. Developments in the field of information and telecommunications in the context of international security / Report of the Secretary General. Fifty-six session. 3 July, 2010. United Nations. A/56/164.

60. Thompson, D. The Democratic Citizen : Social Science and Democratic Theory in the Twentieth century / D. Thompson. – Cambridge: Cambridge Univ. Press, 1970. – 273 p.

ДОДАТКИ

Додаток А

			КОДИ
		Дата(рік, місяць, число)	2019 | 01 | 01
Підприємство	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ ІНКОМ-ІНВЕСТ	за ЄДРПОУ	32068777
Територія		за КОАТУУ	
Організаційно-правова форма господарювання	Товариство з обмеженою відповідальністю	за КОПФГ	
Вид економічної діяльності	68.20 Оренда і управління власною або орендованої нерухомістю	за КВЕД	
Середня кількість працівників	2		
Адреса	03057, м. Київ, Соломянський район, вул.. Смоленська, буд. 31-33		

Баланс на 31.12.2018 р.

Форма № 1-м

Актив	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	2	3	4
I. Необоротні активи			
Незавершені капітальні інвестиції	1005	0	0
Основні засоби:	1010	312.5	300.7
- первісна вартість	1011	851.5	840
- знос	1012	(539)	(539.3)
Довгострокові біологічні активи:	1020	0	0
Довгострокові фінансові інвестиції	1030	0	0
Інші необоротні активи	1090	0	0
Усього за розділом I	**1095**	312.5	300.7
II. Оборотні активи			
Запаси	1100	1930.1	2271.7
- у тому числі готова продукція	1103	1927.2	2268.8
Поточні біологічні активи	1110	0	0
Дебіторська заборгованість за товари, роботи, послуги:	1125	37.9	27.4
Дебіторська заборгованість за розрахунками з бюджетом	1135	0	0.7
- у тому числі податок на прибуток	1136	0	0
Інша поточна дебіторська заборгованість	1155	4.8	39.6
Поточні фінансові інвестиції	1160	0	0
Гроші та їх еквіваленти	1165	0.5	31.8
Витрати майбутніх періодів	1170	0	0
Інші оборотні активи	1190	3.9	0

Усього за розділом II	**1195**	1977.2	2371.2
III. Необоротні активи, утримувані для продажу, та групи вибуття	**1200**	0	0
Баланс	**1300**	2289.7	2671.9

Пасив	**Код рядка**	**На початок звітного періоду**	**На кінець звітного періоду**
1	**2**	**3**	**4**
I. Власний капітал			
Зареєстрований (пайовий) капітал	1400	98.1	98.1
Додатковий капітал	1410	275.8	275.8
Резервний капітал	1415	14.7	14.7
Нерозподілений прибуток (непокритий збиток)	1420	1389.3	1754.1
Неоплачений капітал	1425	(0)	(0)
Усього за розділом I	**1495**	1777.9	2142.7
II. Довгострокові зобов'язання, цільове фінансування та забезпечення	**1595**	0	0
III. Поточні зобов'язання			
Короткострокові кредити банків	1600	152.4	0
Поточна кредиторська заборгованість за: довгостроковими зобов'язаннями	1610	0	0
- товари, роботи, послуги	1615	266.4	372.3
розрахунками з бюджетом	1620	68.1	63.9
у тому числі з податку на прибуток	1621	60	31.1
- зі страхування	1625	5.4	12.4
- з оплати праці	1630	19.5	44.6
Доходи майбутніх періодів	1665	0	0
Інші поточні зобов'язання	1690	0	36
Усього за розділом III	**1695**	511.8	529.2
IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу та групами вибуття	**1700**	0	0
Баланс	**1900**	2289.7	2671.9

Керівник
Головний бухгалтер

Додаток Б

			КОДИ
		Дата(рік, місяць, число)	2019 | 01 | 01
Підприємство	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ ІНКОМ-ІНВЕСТ	за ЄДРПОУ	32068777
Територія		за КОАТУУ	
Організаційно-правова форма господарювання	Товариство з обмеженою відповідальністю	за КОПФГ	
Вид економічної діяльності	68.20 Оренда і управління власною або орендованої нерухомістю	за КВЕД	
Середня кількість працівників	2		
Адреса	03057, м. Київ, Соломянський район, вул.. Смоленська, буд. 31-33		

Звіт про фінансові результати за 2018 р.

Форма № 2-м

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	**2**	**3**	**4**
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	7002.1	5722
Інші операційні доходи	2120	(216.2)	(157.4)
Інші доходи	2240	10.2	0
Разом доходи (2000 + 2120 + 2240)	**2280**	7228.5	5879.4
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(5248.3)	(4344.5)
Інші операційні витрати	2180	(1535.3)	(1201.5)
Інші витрати	2270	(0)	(0)
Разом витрати (2050 + 2180 + 2270)	2285	(6783.6)	(5546)
Фінансовий результат до оподаткування (2268 - 2285)	2290	(444.9)	(333.4)
Податок на прибуток	2300	(80.1)	(60)
Чистий прибуток (збиток) (2290 - 2300)	2350	364.8	273.4

Керівник
Головний бухгалтер

Додаток В

			КОДИ
		Дата(рік, місяць, число)	2018 | 01 | 01
Підприємство	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ ІНКОМ-ІНВЕСТ	за ЄДРПОУ	32068777
Територія		за КОАТУУ	
Організаційно-правова форма господарювання	Товариство з обмеженою відповідальністю	за КОПФГ	
Вид економічної діяльності	68.20 Оренда і управління власною або орендованої нерухомістю	за КВЕД	
Середня кількість працівників	2		
Адреса	03057, м. Київ, Соломянський район, вул.. Смоленська, буд. 31-33		

1. Баланс на 31.12.2017 р.

Форма № 1-м

Актив	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	**2**	**3**	**4**
I. Необоротні активи			
Незавершені капітальні інвестиції	1005	0	0
Основні засоби:	1010	324.5	312.5
- первісна вартість	1011	841.3	851.5
- знос	1012	(516.8)	(539)
Довгострокові біологічні активи:	1020	0	0
Довгострокові фінансові інвестиції	1030	0	0
Інші необоротні активи	1090	0	0
Усього за розділом I	**1095**	324.5	312.5
II. Оборотні активи			
Запаси	1100	1456.5	1930.1
- у тому числі готова продукція	1103	1453.5	1927.2
Поточні біологічні активи	1110	0	0
Дебіторська заборгованість за товари, роботи, послуги:	1125	0	37.9
Дебіторська заборгованість за розрахунками з бюджетом	1135	5	0
- у тому числі податок на прибуток	1136	0	0
Інша поточна дебіторська заборгованість	1155	6.8	4.8
Поточні фінансові інвестиції	1160	0	0
Гроші та їх еквіваленти	1165	10.6	0.5
Витрати майбутніх періодів	1170	0	0
Інші оборотні активи	1190	0	3.9

Усього за розділом II	**1195**	1478.9	1977.2
III. Необоротні активи, утримувані для продажу, та групи вибуття	**1200**	0	0
Баланс	**1300**	1803.4	2289.7

Пасив	**Код рядка**	**На початок звітного періоду**	**На кінець звітного періоду**
1	**2**	**3**	**4**
I. Власний капітал			
Зареєстрований (пайовий) капітал	1400	98.1	98.1
Додатковий капітал	1410	275.8	275.8
Резервний капітал	1415	14.7	14.7
Нерозподілений прибуток (непокритий збиток)	1420	1111.4	1389.3
Неоплачений капітал	1425	(0)	(0)
Усього за розділом I	**1495**	1500	1777.9
II. Довгострокові зобов'язання, цільове фінансування та забезпечення	**1595**	0	0
III. Поточні зобов'язання			
Короткострокові кредити банків	1600	0	152.4
Поточна кредиторська заборгованість за: довгостроковими зобов'язаннями	1610	0	0
- товари, роботи, послуги	1615	196.8	266.4
розрахунками з бюджетом	1620	79.2	68.1
у тому числі з податку на прибуток	1621	0	60
- зі страхування	1625	9.1	5.4
- з оплати праці	1630	17.6	19.5
Доходи майбутніх періодів	1665	0	0
Інші поточні зобов'язання	1690	0.7	0
Усього за розділом III	**1695**	303.4	511.8
IV. Зобов»язання, пов»язані з необоротними активами, утримуваними для продажу та групами вибуття	**1700**	0	0
Баланс	**1900**	1803.4	2289.7

Керівник
Головний бухгалтер

Додаток Г

			КОДИ
		Дата(рік, місяць, число)	2018 | 01 | 01
Підприємство	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ ІНКОМ-ІНВЕСТ	за ЄДРПОУ	32068777
Територія		за КОАТУУ	
Організаційно-правова форма господарювання	Товариство з обмеженою відповідальністю	за КОПФГ	
Вид економічної діяльності	68.20 Оренда і управління власною або орендованої нерухомістю	за КВЕД	
Середня кількість працівників	2		
Адреса	03057, м. Київ, Соломянський район, вул.. Смоленська, буд. 31-33		

Звіт про фінансові результати за 2017 р.

Форма № 2-м

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	**2**	**3**	**4**
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	5722	4335.3
Інші операційні доходи	2120	(0)	(0)
Інші доходи	2240	157.4	144.7
Разом доходи (2000 + 2120 + 2240)	**2280**	5879.4	4480
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(4344.5)	(3018.5)
Інші операційні витрати	2180	(1201.5)	(948.7)
Інші витрати	2270	(0)	(0)
Разом витрати (2050 + 2180 + 2270)	2285	(5546)	(3967.2)
Фінансовий результат до оподаткування (2268 - 2285)	2290	(333.4)	(512.8)
Податок на прибуток	2300	(60)	(80.3)
Чистий прибуток (збиток) (2290 - 2300)	2350	273.4	432.5

Керівник
Головний бухгалтер